

APPROVAL SHEET

Title of Dissertation: Amplified Quantum Transforms

Name of Candidate: David Jonathan Cornwell

Doctor of Philosophy, 2014

Dissertation and Abstract Approved: _____

Dr. S. Lomonaco

Professor

CSEE

Date Approved: _____

CURRICULUM VITAE

1980 Bachelor of Science, Mathematics, University of York, UK

1995 Master of Science, Statistics, UMBC, USA

2014 Doctor of Philosophy, Applied Mathematics, UMBC, USA

ABSTRACT

Title of dissertation: Amplified Quantum Transforms

David J. Cornwell, Doctor of Philosophy
2014

Dissertation directed by: Professor Samuel J. Lomonaco
Department of Computer Science
UMBC

In this thesis we investigate two new Amplified Quantum Transforms. In particular we create and analyze the Amplified Quantum Fourier Transform (Amplified-QFT) and the Amplified-Haar Wavelet Transform. The Amplified-QFT algorithm is used to solve the following problem:

The Local Period Problem: *Let $L = \{0, 1, \dots, N - 1\}$ be a set of N labels and let A be a subset of M labels of period P , i.e. a subset of the form*

$$A = \{j : j = s + rP, r = 0, 1, \dots, M - 1\}$$

where $P \leq \sqrt{N}$ and $M \ll N$, and where M is assumed known. Given an oracle

$$f : L \rightarrow \{0, 1\}$$

which is 1 on A and 0 elsewhere, find the local period P and the offset s .

First, we provide a brief history of quantum mechanics and quantum computing.

Second, we examine the Amplified-QFT in detail and compare it against the Quantum Fourier Transform (QFT) and Quantum Hidden Subgroup (QHS) algorithms for solving the Local Period Problem. We calculate the probabilities of success of each algorithm and show the Amplified-QFT is quadratically faster than the QFT and QHS algorithms.

Third, we examine the Amplified-QFT algorithm for solving The Local Period Problem with an Error Stream.

Fourth, we produce an uncertainty relation for the Amplified-QFT algorithm.

Fifth, we show how the Amplified-Haar Wavelet Transform can solve the Local Constant or Balanced Signal Decision Problem which is a generalization of the Deutsch-Jozsa algorithm.

AMPLIFIED QUANTUM TRANSFORMS

by

David J. Cornwell

2014

Dissertation submitted to the Faculty of the Graduate School of the
University of Maryland, Baltimore County in partial fulfillment
of the requirements for the degree of
Doctor of Philosophy
2014

Advisory Committee:

Professor Samuel J. Lomonaco, Chair/Advisor

Professor Thomas Armstrong, Co-Advisor

Professor Muddappa Gowda

Professor Florian Potra

Professor Yanhua Shih

© Copyright by David J. Cornwell 2014

Acknowledgements

I would like to thank my parents for supporting my university education. I would like to thank my fiancée, Ivone de Lima, for being so considerate while I worked on my PhD since 2006. I would like to wish my three sons, Tim, Zac and Nic a terrific future.

I would also like to express a deep thank you to my thesis advisor Dr Lomonaco. It has been a great pleasure discussing ideas and working closely with him over the years. Also I would like to thank the UMBC Math Department for enabling my cross disciplinary PhD to occur and allowing me to work on my PhD over so many years while I worked full time. This has been a terrific experience.

Table of Contents

List of Abbreviations	iv
1 Introduction	1
1.1 Executive Summary	1
1.2 A Brief History of Quantum Mechanics	5
1.3 A Brief History Of Quantum Computing	9
1.4 Outline of Thesis - Amplified Quantum Transforms	11
2 The Amplified Quantum Fourier Transform	13
2.1 Introduction	13
2.2 Background-Amplitude Amplification	14
2.3 Background-Period Finding	16
2.4 The Amplified Quantum Fourier Transform Algorithm	17
2.5 The QFT Algorithm	19
2.6 The QHS Algorithm	20
2.7 Summary of the Main Results	21
2.8 The Amplified-QFT is Quadratically Faster than the QFT or the QHS	25
2.9 The Amplified-QFT Algorithm - Detailed Analysis	28
2.9.1 Amplified-QFT Analysis: $y=0$	31
2.9.2 Amplified-QFT Analysis: $Py = 0 \bmod N, y \neq 0$	31
2.9.3 Amplified-QFT Analysis: $Py \neq 0 \bmod N$	33
2.9.4 Amplified-QFT Summary	34
2.10 The QFT Algorithm - Detailed Analysis.	34
2.10.1 QFT Analysis: $y = 0$	36
2.10.2 QFT Analysis: $Py = 0 \bmod N, y \neq 0$	36
2.10.3 QFT Analysis: $Py \neq 0 \bmod N$	38
2.10.4 QFT Summary	40
2.11 The QHS Algorithm - Detailed Analysis	40
2.11.1 QHS Analysis: $y = 0$	42
2.11.2 QHS Analysis: $Py = 0 \bmod N, y \neq 0$	42
2.11.3 QHS Analysis: $Py \neq 0 \bmod N$	44
2.11.4 QHS Summary	45

2.12	Recovering the Period P and the Offset s	46
2.12.1	Testing if $P_1 = P$ when s is known or is 0	47
2.12.2	Testing if $(s_1, P_1) = (s, P)$ when s is from a small known set and $s \neq 0$	48
2.12.3	Finding $s \neq 0$ using a Quantum Computer	49
2.13	Replacing the QFT With a General Unitary Transform U	53
2.14	General Amplification Procedure With General Oracle	55
3	The Amplified Quantum Fourier Transform - With Error Stream	59
3.1	Introduction	59
3.2	Comparison of Results Between $L=0$ and $L>0$	64
3.3	The Three Step Amplified-QFT algorithm	85
3.4	Analysis of the Amplified-QFT Algorithm	86
3.4.1	Amplified-QFT Analysis: $y = 0$	88
3.4.2	Amplified-QFT Analysis: $Py = 0 \bmod N, y \neq 0$	89
3.4.3	Amplified-QFT Analysis: $Py \neq 0 \bmod N$	90
3.4.4	Amplified-QFT Summary	92
3.5	Applying the QFT to the Oracle.	92
3.5.1	QFT Analysis: $y = 0$	94
3.5.2	QFT Analysis: $Py = 0 \bmod N, y \neq 0$	94
3.5.3	QFT Analysis: $Py \neq 0 \bmod N$	95
3.5.4	QFT Summary	97
3.6	Applying the QHS to the Oracle	97
3.6.1	QHS Analysis: $y = 0$	99
3.6.2	QHS Analysis: $Py = 0 \bmod N, y \neq 0$	99
3.6.3	QHS Analysis: $Py \neq 0 \bmod N$	100
3.6.4	QHS Summary	102
4	An Uncertainty Principle for the Amplified-QFT	103
5	The Amplified-Haar Wavelet Transform	109
5.1	Introduction	109
5.2	The Local Constant or Balanced Signal Decision Problem- Analysis	112
6	REFERENCES	118

List of Abbreviations

QFT	Quantum Fourier Transform
QHS	Quantum Hidden Subgroup
Amplified-QFT	Amplified Quantum Fourier Transform

Chapter 1: Introduction

1.1 Executive Summary

In this thesis we analyze two new quantum algorithms. The first algorithm is called the Amplified Quantum Fourier Transform (Amplified-QFT) which solves the Local Period Problem (see Chapter 2) and the Local Period Problem with Error Stream (see Chapter 3). We also produce an Uncertainty Principle for this algorithm (see Chapter 4). The second algorithm is called the Amplified Haar Wavelet Transform which solves the **Local Constant or Balanced Signal Decision Problem** which is a generalization of the Deutsch-Josza problem (See Chapter 5).

What is the Local Period Problem? This is best explained by an example. Suppose we have a 1024 long signal of zeros and ones in positions 0 to 1023 which is nearly all zeros, except for 7 ones, which are located at positions {208,213,218,223,228,233,238}. We can see that this sequence of ones has period 5.

The Local Period Problem, is given the signal (which we call an Oracle) and given the number of ones (7), find the period (5) and the starting position of the sequence (the offset 208). In the notation of Chapter 2 we have $N = 1024$, $M = 7$, $P = 5$, $s = 208$ and the periodic set of ones $A = \{208, 213, 218, 223, 228, 233, 238\}$.

How does the Amplified-QFT solve this problem? We begin with a superposi-

tion which has amplitudes of $+1/\sqrt{N}$ where the oracle is zero and $-1/\sqrt{N}$, where the oracle is a one. We then run Grover's algorithm which increases the amplitudes on the positions of the ones given by the set A to very close to $1/\sqrt{M}$, and decreases the amplitudes on the positions of the zeros to very close to 0. We then run the QFT algorithm on this state and make a measurement to try to recover the period P .

Result 1: We show that the Amplified-QFT algorithm is, on average, **quadratically faster** than two other algorithms, the Quantum Fourier Transform (QFT) and the Quantum Hidden Subgroup (QHS) algorithms for solving this problem. This result is obtained in section 2.8. The reason for this is that the QFT and QHS algorithms do not amplify the amplitudes on the set A whereas the Amplified-QFT algorithm does. The results of both the QFT and QHS algorithms are dominated by the number of zeros and so find it difficult to find the period of the small set of ones. For these two algorithms the probability of measuring the value zero is close to 1.

Result 2: We find the probabilities of success of each of these three algorithms. These results are summarized for each of the algorithms in section 2.7 but are obtained in sections 2.9 for the Amplified-QFT, 2.10 for the QFT and 2.11 for the QHS algorithms. We show that the ratio of the probabilities of success of the Amplified-QFT to the QFT algorithms is approximately $N/4M$ whereas the ratio of the probabilities of success of the Amplified-QFT to the QHS algorithms is approximately $N/2M$.

Result 3: In section 2.12 we produce two quantum algorithms for finding the

offset s .

Result 4: In section 2.13 we produce a general result where we replace the QFT by a general unitary operator U in the Amplified-QFT algorithm. We find a property on U such that the ratio of the probabilities of the Amplified-U divided by U case is the same as the ratio of the Amplified-QFT divided by QFT case.

Result 5: In section 2.14, we replace Grover's algorithm with a general amplification algorithm in the Amplified-QFT algorithm and find an upper bound on the probabilities of success in this case.

What is the Local Period Problem with Error Stream? We extend the example described at the beginning of this executive summary.

Suppose, in addition to the 7 ones in the periodic set A , there are $L = 6$ additional ones introduced in random positions due to errors in the oracle. We now have a random set $G = \{17, 111, 234, 433, 727, 813\}$. How does this affect the probability of success for the same three algorithms defined in chapter 2 and the ability to recover the period 5?

Result 6: In chapter 3 section 3.1, we summarize the exact probabilities of success which now include components of sums over a random set. These values are obtained in sections 3.4, 3.5 and 3.6.

Result 7: In section 3.2, we calculate the corresponding expected values and variances of the sums over the random set given by (where $T = L + M$)

$$\left| \frac{M}{T} \omega^{sy} + \frac{1}{T} \sum_{z \in G} \omega^{zy} \right|^2$$

and

$$\left| \frac{1}{T} \omega^{sy} \left[\frac{1 - \omega^{MPy}}{1 - \omega^{Py}} \right] + \frac{1}{T} \sum_{z \in G} \omega^{zy} \right|^2$$

and

$$\left| \frac{1}{T} \sum_{z \in G} \omega^{zy} \right|^2$$

Result 8: Also in section 3.2, for the Amplified-QFT algorithm, we show that an upper bound of the expected probability of success has a minimum value when $L = MinL$ given by

$$MinL = -M^2 + \sqrt{M(M-1)(M(M-1) + N)}$$

This indicates that as L increases to $MinL$, the upper bound of the expected probability of success decreases, but then as L increases in value past $MinL$, the expected probability of success can increase again due to randomness.

Result 9: In chapter 4 we obtain an uncertainty principle for the Amplified-QFT algorithm. Let N = total number of elements, M = number of elements whose amplitudes are close to $1/\sqrt{M}$ after first running Grover's algorithm, N_y = number of elements which have non-zero amplitudes after running the QFT, then we have

$$MN_y \geq N$$

What is the **Local Constant or Balanced Signal Decision Problem**?

This is best explained by an example. Suppose we have a signal S which is 1024 long consisting of zeros and ones. Suppose we are given two pairs of locations $A_{128} = \{128, 129\}$ and $A_{722} = \{722, 723\}$ where the signal is either constant or balanced at these locations and we wish to determine which is the case. Here

$A = A_{128} \cup A_{722}$. For example we could have the constant signal case $S(128) = 0, S(129) = 0, S(722) = 1, S(723) = 1$ or we have a balanced signal case $S(128) = 0, S(129) = 1, S(722) = 1, S(723) = 0$.

Result 10: In chapter 5 section 5.2, we show that the Amplified-Haar Wavelet Transform can solve this problem quadratically faster than a classical algorithm to solve this problem.

Result 11: In general this problem cannot be solved by the Quantum Haar Wavelet Transform alone because the values of the signal on the set \overline{A} (the complementary set of A) affect the results. We do need the amplification step in order to solve this problem. However we identify a specific case where the Quantum Haar Wavelet Transform can solve the problem (when either we have A is constant and \overline{A} is balanced or A is balanced and \overline{A} is constant). We show that in this case, the Amplified-Haar Wavelet Transform is faster than the Quantum Haar-Wavelet transform when $M > \frac{N^{1/3}(1-2M/N)^{4/3}}{2592^{1/3}(1-M/N)^{2/3}}$.

1.2 A Brief History of Quantum Mechanics

In this section we provide a brief history of quantum mechanics (see the list of books in the references section especially books 1, 5, 14, 18, 19, 27, 29, 36 and 37).

As a material body is heated it emits radiation at different frequencies and intensities as the temperature increases. The problem is to provide a theoretical explanation for the observed effects. Rayleigh and Jeans applied the principles of statistical mechanics to this problem but were not completely successful. Their

theoretical models predicted the "Ultraviolet Catastrophe" which did not occur in practice. In 1900 Max Planck solved this black body radiation problem by assuming that the energy of the emitted radiation comes in energy packets or quanta and that the relationship between energy E and frequency ν is given by

$$E = h\nu$$

and where h is Planck's constant where $h = 6.626 \times 10^{-34} Js$. This assumption led him to produce results for the black body radiation problem that matched experimentally observed values which had not been done before. In 1918 he received the Nobel prize for this work.

In 1905 Einstein explained the photo electric effect by using Planck's quantum approach. Light incident on a metal surface causes the emission of electrons. The more intense the light, the more electrons of a given energy are produced. Also light must exceed a certain minimum frequency before electrons are emitted. Einstein produced the following formula for the photo electric effect

$$K = h(\nu - \nu_0)$$

where ν_0 is the frequency of light below which the photo electric effect does not occur, and K is the energy of the emitted electron. Once again, this approach agrees with experimentally observed results.

Around this same timeframe the model of the atom was provided by J.J. Thomson. He had shown by experiment that atoms consist of positively and negatively charged components. His model assumed that the positive charge was distributed

evenly throughout the atom, interspersed with negatively charged electrons. However this classical model could not explain the line spectra of different elements. Rutherford performed experiments concerning the scattering of alpha particles by atoms. His experiments suggested that negatively charged electrons orbited a central positively charged nucleus much like planets orbiting the Sun, however problems remained. Orbiting electrons should emit radiation and fall into the nucleus. The atom should only exist for a very short time.

Niels Bohr decided that a model based on the quantum approach was needed. Suppose the different energy levels of an atom are given by E_1, E_2, \dots then the difference between these energy levels should be discrete values given by

$$h\nu_{m,n} = E_m - E_n$$

where $\nu_{m,n}$ is the frequency of light emitted when the atom moves from the excited state E_m to E_n . The observed line spectra could be explained using the formula

$$E_n = -\frac{Rh}{n^2}$$

By assuming the electrons moved in a circular orbit and the electrostatic attraction force was balanced by the centrifugal force, Bohr was able to obtain a theoretical value for R from the formula

$$R = \frac{4\pi^2 e^4 m_e}{h^3}$$

which agreed with observation (where e is the charge of the electron and m_e is its mass). Sommerfeld extended this work to the case of elliptical orbits. Bohr's

theory of the atom was successful and he created an institute in Copenhagen for atomic studies.

In 1926 Schrodinger developed his famous wave equation which he used to explain the spectral lines of the Hydrogen atom. This equation has the following general form for the time dependent case

$$i\hbar\frac{\partial}{\partial t}\Psi = H\Psi$$

where H is the Hamiltonian operator and Ψ is the state vector or wave function of the system. The wave equation introduces the fundamental concept of superposition for if Ψ_1 is a solution and Ψ_2 is a solution then $\Psi_1 + \Psi_2$ is also a solution by linearity.

Heisenberg developed his matrix mechanics formulation of quantum mechanics which was shown to be equivalent to Schrodinger's wave equation version. Heisenberg also discovered his famous Uncertainty Principle which is a relationship between two complementary or conjugate variables such as position and momentum.

$$\sigma_x\sigma_p \geq \frac{\hbar}{2}$$

where σ is the standard deviation of the appropriate variable.

The Copenhagen Interpretation of quantum mechanics was put forward by Niels Bohr. This contained the elements of unreality, non-locality and uncertainty. Einstein challenged these principles in an ongoing and great debate with Niels Bohr at the 1927 and 1930 Solvay Conferences culminating in the famous Einstein, Podolsky and Rosen (EPR) paper of 1935. In this paper EPR claimed that quantum mechanics should have the elements of reality, locality and certainty which could be achieved by a Hidden Variable theory - a classical theory. However in 1964 John Bell

showed that certain correlations in quantum theory would be much stronger than those of a hidden variable theory and he produced Bell's Inequality which would identify which theory was true. This meant that one could tell from performing an experiment whether quantum mechanics was the correct theory or whether a hidden variable theory was the correct theory. Many experiments have been performed that show quantum mechanics is the true theory and have ruled out most hidden variable theories. However each experiment performed so far has not ruled out all hidden variable theories. Some loopholes have remained. In the future experiments will be performed that will eventually rule out all the remaining loopholes but if we apply the induction argument for theories we can say the probability that quantum mechanics is true is currently very close to 1 and the probability that there is a true hidden variable theory is very close to 0. Alternatively if we use Karl Popper's approach we would say that the theory of quantum mechanics has not been refuted. However there is still the chance it could be refuted in favor of a conjectured hidden variable theory.

1.3 A Brief History Of Quantum Computing

In this section we provide a brief history of the development of quantum computing to set the stage for this thesis.

The early days of quantum computing were kicked off with ideas from Paul Benioff and Richard Feynman. Benioff investigated the idea of whether quantum systems could efficiently simulate classical computers. In 1981 Richard Feynman

investigated the question whether a classical computer could simulate a classical or quantum system exactly. In 1985 Feynman investigated the notions of reversibility and irreversibility in computation.

Then in 1985 David Deutsch wrote a ground breaking paper entitled "Quantum Theory, the Church-Turing Principle and the Universal Quantum Computer", in the Proceedings of the Royal Society in which he replaced Turing's classical ideas of computation with quantum ideas. Quantum computing was born. Deutsch also presented the first quantum algorithm using two qubits, Deutsch's algorithm which was slightly faster than a classical computer.

In 1992, David Deutsch and Richard Josza produced their Deutsch-Josza algorithm that worked on n qubits. The idea is to be able to distinguish whether a Boolean function is balanced or constant. Classically this would take a work factor of 2^n however the quantum algorithm produced an exponential speedup.

In 1994 Peter Shor published a paper entitled "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer" that specified a quantum algorithm to factor large integers using the quantum Fourier transform that was exponentially faster than classical methods. He also described a quantum algorithm to solve the discrete log problem. Factoring and the discrete log problem are at the heart of cryptographic algorithms that are used to protect internet traffic. If you can easily factor numbers then you can break the RSA encryption algorithm. If you can easily solve the discrete log problem then you can easily break the Diffie-Hellman key exchange method. Shor's paper ignited research and global interest in quantum computing, both in the unclassified and classified

arenas. The race is now on to be the first nation to build a real quantum computer that could implement either of these attacks.

In 1996 Lov Grover wrote a paper entitled "A fast quantum mechanical algorithm for database search" in which he described a quantum algorithm that could search for an item in an N long list with a work factor of $O(\sqrt{N})$ providing a quadratic speedup over the classical $O(N)$ method. It was later shown by Zalka (ref 158.) that this algorithm was optimal.

Since Shor's algorithm and Grover's algorithm were published there has been significant research in the area of quantum computing algorithms. There are several good survey articles on the quant-ph website.

1.4 Outline of Thesis - Amplified Quantum Transforms

The two main algorithms of quantum computing are Grover's search algorithm and Shor's algorithm for factoring $n = pq$ by using the quantum Fourier transform. In this thesis we combine Grover's search algorithm with the quantum Fourier transform to solve the Local Period Problem. We call this new algorithm The Amplified Quantum Fourier Transform (Amplified-QFT). We show that this new algorithm solves the Local Period Problem quadratically faster than the quantum Fourier transform alone.

In Chapter 2 we analyze the Amplified-QFT algorithm when applied to a periodic oracle. We calculate and compare the probabilities of success of the QFT algorithm, the quantum hidden subgroup (QHS) algorithm and the Amplified-QFT

algorithm. The contents of this chapter are based off the published paper ref[14].

In Chapter 3 we analyze the Amplified-QFT when applied to a periodic oracle with an error stream and calculate and compare the probabilities of success of the QFT algorithm, the QHS algorithm and the Amplified-QFT algorithm.

In Chapter 4 we produce an uncertainty principle for the Amplified-QFT algorithm.

In Chapter 5 we show how the one dimensional Amplified Haar Wavelet Transforms can be used to solve a certain decision problem.

Chapter 2: The Amplified Quantum Fourier Transform

2.1 Introduction

In this chapter we create and analyze a new quantum algorithm called the Amplified Quantum Fourier Transform (Amplified-QFT) for solving the following problem:

The Local Period Problem: *Let $L = \{0, 1, \dots, N - 1\}$ be a set of N labels and let A be a subset of M labels of period P , i.e. a subset of the form*

$$A = \{j : j = s + rP, r = 0, 1, \dots, M - 1\}$$

where $P \leq \sqrt{N}$ and $M \ll N$, and where M is assumed known. Given an oracle

$$f : L \rightarrow \{0, 1\}$$

which is 1 on A and 0 elsewhere, find the local period P and the offset s .

The first part of this chapter provides some background information on amplitude amplification, period finding and defines the Amplified-QFT algorithm. The second part of the chapter summarizes the main results and compares the Amplified-QFT algorithm against the Quantum Fourier Transform (QFT) and Quantum Hidden Subgroup (QHS) algorithms when solving the local period problem. It is shown that the Amplified-QFT algorithm is, on average, quadratically faster than both

the QFT and QHS algorithms. The third part of the chapter provides the detailed proofs of the main results, describes the method of recovering P from an observation y and describes the algorithm for finding the offset s . In the final section of the chapter we provide a general result where we replace the QFT with a general unitary operator U and identify what property it must have to produce the same probabilities of success as the QFT.

2.2 Background-Amplitude Amplification

In ref[4] Lov Grover specified a quantum search algorithm that searched for a single marked element x_0 in an N long list L . An oracle $f : L \rightarrow \{0, 1\}$ is used to mark the element such that $f(x_0) = 1$ and f is 0 elsewhere. Grover's quantum algorithm finds the element with a work factor of $O(\sqrt{N})$ whereas on a classical computer this would take $O(N)$, thereby obtaining a quadratic speedup. Grover's algorithm can be summarized as follows:

a) Initialize the state to be the uniform superposition state $|\psi\rangle = H|0\rangle$ where H is the Hadamard transform.

b) Reflect the current state about the plane orthogonal to the state $|x_0\rangle$ by using the operator $(I - 2|x_0\rangle\langle x_0|)$.

c) Reflect the new state back around $|\psi\rangle$ by using the operator $(2|\psi\rangle\langle\psi| - I)$. This operator is a reflection about the average of the amplitudes of the new state.

d) Repeat steps b) and c) $O(\sqrt{N})$ times until most of the probability is on

$|x0\rangle$.

e) Measure the resulting state to obtain $x0$.

Also in ref[4], Grover suggested this algorithm could be extended to the case of searching for an element in a subset A of M marked elements in an N long list L . Once again an oracle $f : L \rightarrow \{0, 1\}$ is used to mark the elements of the subset A . Grover's algorithm solves this problem with a work factor of $O(\sqrt{N/M})$. The elements of the set A are sometimes referred to as "good" and the elements not in A are called "bad". Grover's algorithm for this problem can be summarized as follows:

a) Initialize the state to be the uniform superposition state $|\psi\rangle = H|0\rangle$ where H is the Hadamard transform.

b) Reflect the current state about the plane orthogonal to the state $|x_{good}\rangle$ by using the operator $(I - 2|x_{good}\rangle\langle x_{good}|)$, where $|x_{good}\rangle$ is the normalized sum of the good states defined by the set A . This changes the sign of the amplitudes of the good states defined by A .

c) Reflect the new state back around $|\psi\rangle$ by using the operator $(2|\psi\rangle\langle\psi| - I)$.

d) Repeat steps b) and c) $O(\sqrt{N/M})$ times until most of the probability is on the set A .

e) Measure the resulting state to obtain an element in the set A .

Both versions of Grover's algorithm are also known as Amplitude Amplification algorithms which are generalized even further in ref [9]. The first part of the Amplified-QFT algorithm consists of the second of these algorithms, except for the final measurement step e).

2.3 Background-Period Finding

In ref[3], Peter Shor describes a quantum algorithm to solve the factorization problem with exponential speed up over classical approaches. He translates the factorization problem into one of finding the period of the function $a^x \text{Mod} N$ where N is the number to be factored and $\gcd(a, N) = 1$. The period is found by making use of the QFT. Shor's factorization algorithm is summarized below:

- a) Find $Q : N^2 \leq Q < 2N^2$
- b) Find $a : \gcd(a, N) = 1$
- c) Find the period of $a^x \text{Mod} N$ using the QFT and using the Q th root of unity
 - Form the superposition $\frac{1}{\sqrt{Q}} \sum |x\rangle |a^x \text{Mod} N\rangle$
 - Apply the QFT to the first register $|x\rangle \rightarrow \sum \omega^{xy} |y\rangle$
 - Measure y
 - Form the continued fraction expansion of y/Q to find d/P
 - If $|y/Q - d/P| < 1/2N^2$ and $\gcd(d, P) = 1$ then P is recovered
- d) If the period is not even start over
- e) If $a^{P/2} + 1 = 0 \text{Mod} N$ start over
- f) Find $\gcd(a^{P/2} - 1, N)$ to find the factor of N .

Step c) is the quantum part of Shor's factorization algorithm. We make use of the QFT and continued fraction expansion method to recover the period P in the second part of the Amplified-QFT algorithm.

2.4 The Amplified Quantum Fourier Transform Algorithm

The Amplified-QFT algorithm solves the Local Period Problem:

The Local Period Problem: Let $L = \{0, 1, \dots, N - 1\}$ be a set of N labels and let A be a subset of M labels of period P , i.e. a subset of the form

$$A = \{j : j = s + rP, r = 0, 1, \dots, M - 1\}$$

where $P \leq \sqrt{N}$ and $M \ll N$, and where M is assumed known. Given an oracle

$$f : L \rightarrow \{0, 1\}$$

which is 1 on A and 0 elsewhere, find the local period P and the offset s .

The Amplified-QFT algorithm consists of the following steps where steps a) through d) are the Amplitude Amplification steps and steps e) through i) are the period finding steps that use the QFT:

a) Initialize the state to be the uniform superposition state $|\psi\rangle = H|0\rangle$ where H is the Hadamard transform.

b) Reflect the current state about the plane orthogonal to the state $|x_{good}\rangle$ by using the operator $(I - 2|x_{good}\rangle\langle x_{good}|)$, where $|x_{good}\rangle$ is the normalized sum of the good states defined by the set A . This changes the sign of the amplitudes of the good states defined by A .

c) Reflect the new state back around $|\psi\rangle$ by using the operator $(2|\psi\rangle\langle\psi| - I)$.

d) Repeat steps b) and c) $O(\sqrt{N/M})$ times until most of the probability is on the set A .

- e) Apply the QFT to the resulting state
- f) Make a measurement y
- g) Form the continued fraction expansion of y/N to find d/P
- h) If $|y/N - d/P| < 1/2P^2$ and $\gcd(d, P) = 1$ then P is recovered
- i) If $\gcd(d, P) \neq 1$ repeat the algorithm starting at step a)

The Amplified-QFT algorithm produces the following states (See later sections for the detailed analysis of the Amplified-QFT algorithm):

After applying steps b) and c) k times where $k = \left\lfloor \frac{\pi}{4 \sin^{-1}(\sqrt{M/N})} \right\rfloor$ we arrive at the following state:

$$|\psi_k\rangle = a_k \sum_{z \in A} |z\rangle + b_k \sum_{z \notin A} |z\rangle$$

where

$$a_k = \frac{1}{\sqrt{M}} \sin(2k+1)\theta, b_k = \frac{1}{\sqrt{N-M}} \cos(2k+1)\theta$$

are the appropriate amplitudes of the states and where the angle θ is given by

$$\sin \theta = \sqrt{M/N}, \cos \theta = \sqrt{1 - M/N}$$

.

The QFT at step e) performs the following action

$$|z\rangle \rightarrow \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} e^{-2\pi i z y / N} |y\rangle$$

After the application of the QFT to the state $|\psi_k\rangle$, letting $\omega = e^{-2\pi i / N}$ we

arrive at the following state:

$$|\phi_k\rangle = \sum_{y=0}^{N-1} \left[\frac{a_k}{\sqrt{N}} \sum_{z \in A} \omega^{zy} + \frac{b_k}{\sqrt{N}} \sum_{z \notin A} \omega^{zy} \right] |y\rangle$$

.

At step f) we measure this state with respect to the standard basis to yield an integer $y \in \{0, 1, \dots, N-1\}$ from which we can determine the period P using the continued fraction method.

In a later section where we summarize the main results, we provide a table showing the probabilities of measuring y for the Amplified-QFT algorithm and compare them against the probabilities obtained by performing the QFT and QHS algorithms.

2.5 The QFT Algorithm

The QFT algorithm applied to the Local Period Problem does not include the amplitude amplification steps and consists of the following steps:

- a) Initialize the state to be the uniform superposition state $|\psi\rangle = H|0\rangle$ where H is the Hadamard transform.
- b) Apply the oracle f to $|\psi\rangle$
- c) Apply the QFT to this state
- d) Make a measurement y
- e) Form the continued fraction expansion of y/N to find d/P
- f) If $|y/N - d/P| < 1/2P^2$ and $\gcd(d, P) = 1$ then P is recovered
- g) If $\gcd(d, P) \neq 1$ repeat the algorithm starting at step a)

At step b) after applying the oracle the state is given by (See later sections for the detailed analysis of the QFT algorithm):

$$|\psi_1\rangle = \frac{1}{\sqrt{N}} \left[(-2) \sum_{z \in A} |z\rangle + \sum_{z=0}^{N-1} |z\rangle \right]$$

At step c) the QFT applies the following action:

$$|z\rangle \rightarrow \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} \omega^{zy} |y\rangle$$

to get

$$|\psi_2\rangle = \sum_{y=0}^{N-1} \left[\frac{(-2)}{N} \sum_{z \in A} \omega^{zy} + \frac{1}{N} \sum_{z=0}^{N-1} \omega^{zy} \right] |y\rangle$$

At step d) we measure this state with respect to the standard basis to yield an integer $y \in \{0, 1, \dots, N-1\}$ from which we can determine the period P using the continued fraction method. We note that in the QFT algorithm case, we would have to repeat the algorithm many times to recover the period P because as we will see shortly, most of the probability is on the state $|0\rangle$.

2.6 The QHS Algorithm

The QHS algorithm is a two register algorithm and does not include the amplitude amplification steps. It consists of the following steps:

- a) Initialize the state to be the uniform superposition state $|\psi\rangle = H|0\rangle |0\rangle$ where H is the Hadamard transform.
- b) Apply the oracle f and put the result into the second register of $|\psi\rangle$
- c) Apply the QFT to the first register of this state

- d) Make a measurement y
- e) Form the continued fraction expansion of y/N to find d/P
- f) If $|y/N - d/P| < 1/2P^2$ and $\gcd(d, P) = 1$ then P is recovered
- g) If $\gcd(d, P) \neq 1$ repeat the algorithm starting at step a)

At step b) we have the following state (See later sections for the detailed analysis of the QHS algorithm):

$$|\psi_1\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle |f(x)\rangle$$

After applying the QFT the state is given by:

$$|\psi_2\rangle = \sum_{y=0}^{N-1} \frac{1}{N} |y\rangle \sum_{x=0}^{N-1} \omega^{xy} |f(x)\rangle$$

At step d) we measure this state with respect to the standard basis to yield an integer $y \in \{0, 1, \dots, N-1\}$ from which we can determine the period P using the continued fraction method. We note that in the QHS algorithm case, we would have to repeat the algorithm many times to recover the period P because as we will see shortly, most of the probability is on the state $|0\rangle$.

2.7 Summary of the Main Results

We summarize the main results and compare the probability $\Pr(y)$ of measuring y in the final state arrived at for each of the three algorithms: 1) the Amplified-QFT algorithm 2) the QFT algorithm and 3) the QHS algorithm. Here $\sin \theta = \sqrt{M/N}$ and $k = \lfloor \frac{\pi}{4\theta} \rfloor$ and $0 \leq \frac{\sin^2(\pi M P y / N)}{\sin^2(\pi P y / N)} \leq M^2$.

Case 1 (Amplified-QFT):

The probability $\Pr(y)$ is given exactly by

$$\left\{ \begin{array}{ll} \cos^2 2k\theta & \text{if } y = 0 \\ \\ \tan^2 \theta \sin^2 2k\theta & \text{if } Py = 0 \bmod N, y \neq 0 \\ \\ \frac{1}{M^2} \tan^2 \theta \sin^2 2k\theta \frac{\sin^2(\pi MPy/N)}{\sin^2(\pi Py/N)} & \text{if } Py \neq 0 \bmod N \text{ and } MPy \neq 0 \bmod N \\ \\ 0 & \text{if } Py \neq 0 \bmod N \text{ and } MPy = 0 \bmod N \end{array} \right\}$$

Case 2 (QFT):

The probability $\Pr(y)$ is given exactly by

$$\left\{ \begin{array}{ll} \left(1 - \frac{2M}{N}\right)^2 & \text{if } y = 0 \\ \\ 4 \frac{M^2}{N^2} & \text{if } Py = 0 \bmod N, y \neq 0 \\ \\ \frac{4}{N^2} \frac{\sin^2(\pi MPy/N)}{\sin^2(\pi Py/N)} & \text{if } Py \neq 0 \bmod N \text{ and } MPy \neq 0 \bmod N \\ \\ 0 & \text{if } Py \neq 0 \bmod N \text{ and } MPy = 0 \bmod N \end{array} \right\}$$

Case 3 (QHS):

The probability $\Pr(y)$ is given exactly by

$$\left\{ \begin{array}{ll} 1 - \frac{2M(N-M)}{N^2} & \text{if } y = 0 \\ \frac{2M^2}{N^2} & \text{if } Py = 0 \bmod N, y \neq 0 \\ \frac{2}{N^2} \frac{\sin^2(\pi MPy/N)}{\sin^2(\pi Py/N)} & \text{if } Py \neq 0 \bmod N \text{ and } MPy \neq 0 \bmod N \\ 0 & \text{if } Py \neq 0 \bmod N \text{ and } MPy = 0 \bmod N \end{array} \right\}$$

We note that for the QFT and QHS algorithms $\Pr(y = 0)$ is very close to 1 because $M \ll N$. In the cases where $y \neq 0$ we compare the ratios of $\Pr(y)$ in the Amplified-QFT and QFT case and then in the Amplified-QFT and QHS case. Let y be fixed such that either

1. $Py = 0 \bmod N, y \neq 0$ or
2. $Py \neq 0 \bmod N$ and $MPy \neq 0 \bmod N$

and define $\Pr Ratio(y) = \Pr(y)_{\text{Amplified-QFT}} / \Pr(y)_{\text{QFT}}$ then we have the following (see the later detailed sections)

$$\begin{aligned} \frac{N}{4M} \left(\frac{N}{N-M} \right) &\geq \Pr Ratio(y) \geq \frac{N}{4M} \left(\frac{N}{N-M} \right) \left(1 - \frac{2M}{N} \right)^2 \\ &\implies \Pr Ratio(y) \approx \frac{N}{4M} \end{aligned}$$

and define $\Pr Ratio(y) = \Pr(y)_{\text{Amplified-QFT}} / \Pr(y)_{\text{QHS}}$ then we have the following

$$\begin{aligned}\frac{N}{2M}(\frac{N}{N-M}) &\geq \Pr \text{Ratio}(y) \geq \frac{N}{2M}(\frac{N}{N-M})(1 - \frac{2M}{N})^2 \\ &\implies \Pr \text{Ratio}(y) \approx \frac{N}{2M}\end{aligned}$$

Let $S_{ALG} = \{y : |\frac{y}{N} - \frac{d}{P}| \leq \frac{1}{2P^2}, (d, P) = 1\}$ be the set of "successful" y 's.

That is S_{ALG} consists of those y 's which can be measured after applying one of the three algorithms denoted by ALG and from which the period P can be recovered by the method of continued fractions. Note that the set S_{ALG} is the same for each algorithm. However the probability of this set varies with each algorithm. We can see from the following that given y_1 and y_2 , whose probability ratios satisfy the same inequality, we can add their probabilities to get a new ratio that satisfies the same inequality. In this way we can add probabilities over a set on the numerator and denominator and maintain the inequality:

$$\begin{aligned}A &> \frac{P(y_1)}{Q(y_1)} > B \text{ and } A > \frac{P(y_2)}{Q(y_2)} > B \\ &\implies A > \frac{P(y_1) + P(y_2)}{Q(y_1) + Q(y_2)} > B\end{aligned}$$

We see from the cases given above that

$$\frac{N}{4M}(\frac{N}{N-M}) \geq \frac{\Pr(S_{\text{Amplified-QFT}})}{\Pr(S_{QFT})} \geq \frac{N}{4M}(\frac{N}{N-M})(1 - \frac{2M}{N})^2$$

where the difference between the upper bound and lower bound is exactly 1 and that

$$\frac{N}{2M}(\frac{N}{N-M}) \geq \frac{\Pr(S_{\text{Amplified-QFT}})}{\Pr(S_{QHS})} \geq \frac{N}{2M}(\frac{N}{N-M})(1 - \frac{2M}{N})^2$$

where the difference between the upper bound and lower bound is exactly 2.

This shows that the Amplified-QFT is approximately $\frac{N}{4M}$ times more successful than the QFT and $\frac{N}{2M}$ times more successful than the QHS when $M \ll N$. In addition it also shows that the QFT is 2 times more successful than the QHS in this problem. However, the success of the Amplified-QFT algorithms comes at an increase in work factor of $O(\sqrt{\frac{N}{M}})$. We note that in the case that P is a prime number that $(d, P) = 1$ is met trivially. However when P is composite the algorithms may need to be rerun several times until $(d, P) = 1$ is satisfied.

Towards the end of the chapter we show how to test whether a putative value of P , given s is known, can be tested to see if it is the correct value. We also investigate the case where s is unknown but is from a small known set of values such that the values of s can be exhausted over on a classical computer. We also show how s can be recovered by using a quantum algorithm using amplitude amplification followed by a measurement.

2.8 The Amplified-QFT is Quadratically Faster than the QFT or the QHS

We show that the Amplified-QFT algorithm is, on average, quadratically faster than the QFT or QHS algorithms. In order to show this, we use the geometric probability distribution which provides the probability of the first success in a sequence of trials where the probability of success is p and the probability of failure is $1 - p$. For both the QFT and QHS algorithms a trial is one complete execution of the

algorithm. Because the probability of measuring $y = 0$ is close to 1 we expect to have to repeat the algorithm many times due to failure of measuring a successful y , before we have the first success.

If X is the random variable which counts the number of trials until the first success then

$$P(X = k) = (1 - p)^{k-1}p \text{ for } k = 1, 2, \dots$$

The expected value $E[X]$ and variance $Var[X]$ are given by:

$$E[X] = \frac{1}{p} \text{ and } Var[X] = \frac{1 - p}{p^2}$$

The workfactor of the Amplified-QFT algorithm is given by the number of iterations of each amplification step followed by a single QFT step:

$$O(\sqrt{\frac{N}{M}})$$

For the QFT algorithm we have the probability of failure $1 - p$ is given by

$$\Pr(failure) = 1 - p \geq \Pr(y = 0) = (1 - \frac{2M}{N})^2$$

then

$$\Pr(success) = p \leq 1 - (1 - \frac{2M}{N})^2 = \frac{4M}{N}(1 - \frac{M}{N})$$

Then for the QFT algorithm, the expected number of trials until the first success is

$$E[X] = \frac{1}{p} \geq \frac{N}{4M(1 - \frac{M}{N})} \geq \frac{N}{4M}$$

The workfactor of the QFT algorithm is the expected number of times the QFT has to be run, is given approximately by:

$$O(\frac{N}{M})$$

Therefore the ratio of the expected work factor of the QFT algorithm and the work factor of the Amplified-QFT is given by

$$O(\sqrt{\frac{N}{M}})$$

showing that the Amplified-QFT algorithm is, on average, quadratically faster than the QFT algorithm.

The variance in the number of times the QFT algorithm is run is given by

$$Var[X] = \frac{1-p}{p^2} \geq (\frac{N}{N-M})^2 (\frac{N-2M}{4M})^2$$

For the QHS algorithm we have the probability of failure $1-p$ is given by

$$\Pr(failure) = 1-p \geq \Pr(y=0) = 1 - \frac{2M(N-M)}{N^2}$$

then

$$\Pr(success) = p \leq 1 - (1 - \frac{2M(N-M)}{N^2}) = \frac{2M}{N}(1 - \frac{M}{N})$$

Then for the QHS algorithm, the expected number of trials until the first success is

$$E[X] = \frac{1}{p} \geq \frac{N}{2M(1 - \frac{M}{N})} \geq \frac{N}{2M}$$

The workfactor of the QHS algorithm is the expected number of times the QHS has to be run, is given approximately by:

$$O(\frac{N}{M})$$

Therefore the ratio of the expected work factor of the QHS algorithm and the work factor of the Amplified-QFT is given by

$$O(\sqrt{\frac{N}{M}})$$

showing that the Amplified-QFT algorithm is, on average, quadratically faster than the QHS algorithm.

The variance in the number of times the QHS algorithm is run is given by

$$Var[X] = \frac{1-p}{p^2} \geq (\frac{N}{N-M})^2 (\frac{(N-M)^2 + M^2}{4M^2})$$

2.9 The Amplified-QFT Algorithm - Detailed Analysis

In this section we examine the Amplified-QFT algorithm in detail and produce the results for the probability of success that were summarized in an earlier section.

The Amplified-QFT algorithm is defined by the following procedure (see earlier section):

Steps a) to d): Apply the Amplitude Amplification algorithm to the starting state $|0\rangle$. The resulting state is given by $|\psi_k\rangle$ (ref[4], ref[7], ref[1]) where $k =$

$$\left\lfloor \frac{\pi}{4 \sin^{-1}(\sqrt{M/N})} \right\rfloor :$$

$$|\psi_k\rangle = a_k \sum_{z \in A} |z\rangle + b_k \sum_{z \notin A} |z\rangle$$

where

$$a_k = \frac{1}{\sqrt{M}} \sin(2k+1)\theta, b_k = \frac{1}{\sqrt{N-M}} \cos(2k+1)\theta$$

are the appropriate amplitudes of the states and where

$$\sin \theta = \sqrt{M/N}, \cos \theta = \sqrt{1 - M/N}$$

Now we have , ref[7],

$$k = \left\lfloor \frac{\pi}{4\theta} \right\rfloor \implies \frac{\pi}{4\theta} - 1 \leq k \leq \frac{\pi}{4\theta} \implies \frac{\pi}{2} - \theta \leq (2k+1)\theta \leq \frac{\pi}{2} + \theta$$

$$\implies \sin \theta = \cos(\frac{\pi}{2} - \theta) \geq \cos(2k+1)\theta \geq \cos(\frac{\pi}{2} + \theta) = -\sin \theta$$

Notice that the total probability of the N-M labels that are not in A is

$$(N-M) \left(\frac{1}{\sqrt{N-M}} \cos(2k+1)\theta \right)^2 = \cos^2(2k+1)\theta$$

$$\implies \cos^2(2k+1)\theta \leq \sin^2 \theta = \sin^2(\sin^{-1}(\sqrt{\frac{M}{N}}))$$

$$\implies \cos^2(2k+1)\theta \leq \frac{M}{N}$$

whereas the total probability of the M labels in A is

$$M \left(\frac{1}{\sqrt{M}} \sin(2k+1)\theta \right)^2 = \sin^2(2k+1)\theta = 1 - \cos^2(2k+1)\theta$$

$$\implies \sin^2(2k+1)\theta \geq 1 - \frac{M}{N}$$

Step e): Apply the QFT which performs the following action

$$|z\rangle \rightarrow \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} e^{-2\pi i z y / N} |y\rangle$$

After the application of the QFT to the state $|\psi_k\rangle$, letting $\omega = e^{-2\pi i / N}$, we have

$$|\phi_k\rangle = \frac{a_k}{\sqrt{N}} \sum_{z \in A} \sum_{y=0}^{N-1} \omega^{zy} |y\rangle + \frac{b_k}{\sqrt{N}} \sum_{z \notin A} \sum_{y=0}^{N-1} \omega^{zy} |y\rangle$$

After interchanging the order of summation, we have

$$|\phi_k\rangle = \sum_{y=0}^{N-1} \left[\frac{a_k}{\sqrt{N}} \sum_{z \in A} \omega^{zy} + \frac{b_k}{\sqrt{N}} \sum_{z \notin A} \omega^{zy} \right] |y\rangle$$

Steps f) to i): Measure with respect to the standard basis to yield a integer $y \in \{0, 1, \dots, N-1\}$ from which we can determine the period P using the continued fraction method.

The amplitude $Amp(y)$ of $|y\rangle$ is given by

$$\begin{aligned} Amp(y) &= \frac{a_k}{\sqrt{N}} \sum_{z \in A} \omega^{zy} + \frac{b_k}{\sqrt{N}} \sum_{z \notin A} \omega^{zy} \\ &= \frac{(a_k - b_k)}{\sqrt{N}} \sum_{z \in A} \omega^{zy} + \frac{b_k}{\sqrt{N}} \sum_{z=0}^{N-1} \omega^{zy} \\ &= \frac{(a_k - b_k)}{\sqrt{N}} \sum_{r=0}^{M-1} \omega^{(s+rP)y} + \frac{b_k}{\sqrt{N}} \sum_{z=0}^{N-1} \omega^{zy} \quad (\text{A is periodic}) \\ &= \frac{(a_k - b_k)}{\sqrt{N}} \omega^{sy} \sum_{r=0}^{M-1} \omega^{rPy} + \frac{b_k}{\sqrt{N}} \sum_{z=0}^{N-1} \omega^{zy} \end{aligned}$$

We calculate the $\Pr(y)$ for the following cases:

- a) $y = 0$
- b) $P y = 0 \bmod N$ and $y \neq 0$
- c) $P y \neq 0 \bmod N$

2.9.1 Amplified-QFT Analysis: $y=0$

We calculate the probability $\Pr(y = 0)$

$$\begin{aligned}
Amp(y) &= \frac{a_k}{\sqrt{N}} \sum_{z \in A} \omega^{zy} + \frac{b_k}{\sqrt{N}} \sum_{z \notin A} \omega^{zy} \\
&= \frac{1}{\sqrt{N}} (M a_k + (N - M) b_k) \\
&= \frac{1}{\sqrt{N}} \left[\frac{M}{\sqrt{M}} \sin(2k + 1)\theta + \frac{N - M}{\sqrt{N - M}} \cos(2k + 1)\theta \right] \\
&= \sqrt{\frac{M}{N}} \sin(2k + 1)\theta + \sqrt{1 - \frac{M}{N}} \cos(2k + 1)\theta \\
&= \sin \theta \sin(2k + 1)\theta + \cos \theta \cos(2k + 1)\theta \\
&= \cos(2k\theta)
\end{aligned}$$

We have

$$\Pr(y = 0) = \cos^2(2k\theta)$$

2.9.2 Amplified-QFT Analysis: $P y = 0 \bmod N, y \neq 0$

We calculate the probability $\Pr(y)$ in the case where $P y = 0 \bmod N, y \neq 0$

Using the fact that

$$\sum_{z=0}^{N-1} \omega^{zy} = \frac{1 - \omega^{Ny}}{1 - \omega^y} = 0, w^y \neq 1$$

we have

$$\begin{aligned} Amp(y) &= \frac{(a_k - b_k)}{\sqrt{N}} \omega^{sy} \sum_{r=0}^{M-1} \omega^{rPy} + \frac{b_k}{\sqrt{N}} \sum_{z=0}^{N-1} \omega^{zy} \\ &= \frac{(a_k - b_k)}{\sqrt{N}} \omega^{sy} \sum_{r=0}^{M-1} \omega^{rPy} \\ &= \frac{(a_k - b_k)}{\sqrt{N}} \omega^{sy} M \\ &= \frac{Mw^{sy}}{\sqrt{NM}} \sin(2k+1)\theta - \frac{Mw^{sy}}{\sqrt{N(N-M)}} \cos(2k+1)\theta \\ &= \omega^{sy} \sqrt{\frac{M}{N}} (\sin(2k+1)\theta - \sqrt{\frac{M/N}{1-M/N}} \cos(2k+1)\theta) \\ &= \omega^{sy} \sqrt{\frac{M}{N}} (\sin(2k+1)\theta - \frac{\sin \theta}{\cos \theta} \cos(2k+1)\theta) \\ &= \omega^{sy} \tan \theta \sin 2k\theta \end{aligned}$$

We have the probability $\Pr(y)$ in the case where $Py = 0 \pmod{N}, y \neq 0$ is given by

$$\Pr(y) = \tan^2 \theta \sin^2 2k\theta$$

Using $k = \lfloor \frac{\pi}{4\theta} \rfloor \implies \frac{\pi}{4\theta} - 1 \leq k \leq \frac{\pi}{4\theta} \implies \frac{\pi}{2} - 2\theta \leq 2k\theta \leq \frac{\pi}{2} \implies \sin(\frac{\pi}{2} - 2\theta) \leq \sin 2k\theta \leq 1$ we have the following inequality for the probability $\Pr(y)$ in the case where $Py = 0 \pmod{N}, y \neq 0$

$$\begin{aligned} \frac{\sin^2 \theta}{\cos^2 \theta} &\geq \Pr(y) = \tan^2 \theta \sin^2 2k\theta \geq \tan^2 \theta \sin^2(\frac{\pi}{2} - 2\theta) \\ &\implies \frac{M}{N} \frac{1}{1 - \frac{M}{N}} \geq \Pr(y) \geq \tan^2 \theta \sin^2(\frac{\pi}{2} - 2\theta) \\ &\implies \frac{M}{N} (\frac{N}{N-M}) \geq \Pr(y) \geq \frac{\sin^2 \theta}{\cos^2 \theta} \cos^2 2\theta \end{aligned}$$

$$\begin{aligned}
&\Rightarrow \frac{M}{N} \left(\frac{N}{N-M} \right) \geq \Pr(y) \geq \frac{\sin^2 \theta}{\cos^2 \theta} (2 \cos^2 \theta - 1)^2 \\
&\Rightarrow \frac{M}{N} \left(\frac{N}{N-M} \right) \geq \Pr(y) \geq \frac{M}{N} \left(\frac{N}{N-M} \right) \left(1 - \frac{2M}{N} \right)^2
\end{aligned}$$

2.9.3 Amplified-QFT Analysis: $Py \neq 0 \pmod N$

We calculate $\Pr(y)$ in the case where $Py \neq 0 \pmod N$.

Making use of the previous results we have

$$\begin{aligned}
Amp(y) &= \frac{(a_k - b_k)}{\sqrt{N}} \omega^{sy} \sum_{r=0}^{M-1} \omega^{rPy} + \frac{b_k}{\sqrt{N}} \sum_{z=0}^{N-1} \omega^{zy} \\
&= \frac{(a_k - b_k)}{\sqrt{N}} \omega^{sy} \sum_{r=0}^{M-1} \omega^{rPy} \\
&= \frac{(a_k - b_k)}{\sqrt{N}} \omega^{sy} \left[\frac{1 - \omega^{MPy}}{1 - \omega^{Py}} \right] \\
&= \frac{1}{M} \frac{(a_k - b_k)}{\sqrt{N}} \omega^{sy} M \left[\frac{1 - \omega^{MPy}}{1 - \omega^{Py}} \right] \\
&= \frac{1}{M} \omega^{sy} \tan \theta \sin 2k\theta \left[\frac{1 - \omega^{MPy}}{1 - \omega^{Py}} \right]
\end{aligned}$$

Making use of the following identity

$$|1 - e^{i\theta}|^2 = 4 \sin^2(\theta/2)$$

we have

$$\left| \frac{1 - \omega^{MPy}}{1 - \omega^{Py}} \right|^2 = \frac{\sin^2(\pi MPy/N)}{\sin^2(\pi Py/N)}$$

and so the probability $\Pr(y)$ in the case where $Py \neq 0 \pmod N$ is given by

$$\Pr(y) = \frac{1}{M^2} \tan^2 \theta \sin^2 2k\theta \frac{\sin^2(\pi MPy/N)}{\sin^2(\pi Py/N)}$$

Using the previous result $\frac{M}{N} \left(\frac{N}{N-M} \right) \geq \tan^2 \theta \sin^2 2k\theta \geq \frac{M}{N} \left(\frac{N}{N-M} \right) \left(\frac{N-2M}{N} \right)^2$ and letting

$R = \frac{\sin^2(\pi MPy/N)}{\sin^2(\pi Py/N)}$ we have

$$\frac{1}{M^2} \frac{M}{N} \left(\frac{N}{N-M} \right) R \geq \Pr(y) \geq \frac{1}{M^2} \frac{M}{N} \left(\frac{N}{N-M} \right) \left(1 - \frac{2M}{N} \right)^2 R \text{ and so}$$

$$\frac{1}{NM} \left(\frac{N}{N-M} \right) R \geq \Pr(y) \geq \frac{1}{NM} \left(\frac{N}{N-M} \right) \left(1 - \frac{2M}{N} \right)^2 R$$

We notice that if in addition $MPy = 0 \bmod N$ then $\Pr(y) = 0$.

2.9.4 Amplified-QFT Summary

The probability $\Pr(y)$ for the Amplified-QFT is summarized in the following table and is given exactly by

$$\left\{ \begin{array}{ll} \cos^2 2k\theta & \text{if } y = 0 \\ \\ \tan^2 \theta \sin^2 2k\theta & \text{if } Py = 0 \bmod N, y \neq 0 \\ \\ \frac{1}{M^2} \tan^2 \theta \sin^2 2k\theta \frac{\sin^2(\pi MPy/N)}{\sin^2(\pi Py/N)} & \text{if } Py \neq 0 \bmod N \text{ and } MPy \neq 0 \bmod N \\ \\ 0 & \text{if } Py \neq 0 \bmod N \text{ and } MPy = 0 \bmod N \end{array} \right\}$$

2.10 The QFT Algorithm - Detailed Analysis.

In this section we examine the QFT algorithm in detail and produce the results for the probability of success that were summarized earlier in the paper. We just apply the QFT to the binary oracle f , which is 1 on A and 0 elsewhere.

We begin with the following state

$$|\xi\rangle = \frac{1}{\sqrt{N}} \sum_{z=0}^{N-1} |z\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

and apply the unitary transform for f , U_f , to this state which performs the following action:

$$U_f |z\rangle |c\rangle = |z\rangle |c \oplus f(z)\rangle$$

to get the state $|\psi\rangle$

$$\begin{aligned} |\psi\rangle &= U_f \frac{1}{\sqrt{N}} \sum_{z=0}^{N-1} |z\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \\ &= \frac{1}{\sqrt{N}} \left[(-1) \sum_{z \in A} |z\rangle + \sum_{z \notin A} |z\rangle \right] \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \\ &= \frac{1}{\sqrt{N}} \left[(-2) \sum_{z \in A} |z\rangle + \sum_{z=0}^{N-1} |z\rangle \right] \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \end{aligned}$$

Next we apply the QFT to try to find the period P , dropping $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$.

The QFT applies the following action:

$$|z\rangle \rightarrow \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} \omega^{zy} |y\rangle$$

to get

$$|\phi\rangle = \sum_{y=0}^{N-1} \left[\frac{(-2)}{N} \sum_{z \in A} \omega^{zy} + \frac{1}{N} \sum_{z=0}^{N-1} \omega^{zy} \right] |y\rangle$$

We calculate the $\Pr(y)$ for the following cases:

- a) $y = 0$
- b) $Py = 0 \bmod N$ and $y \neq 0$
- c) $Py \neq 0 \bmod N$

2.10.1 QFT Analysis: $y = 0$

We calculate the probability $\Pr(y = 0)$.

We have

$$\begin{aligned}
 \text{Amp}(y) &= \frac{(-2)}{N} \sum_{z \in A} \omega^{zy} + \frac{1}{N} \sum_{z=0}^{N-1} \omega^{zy} \\
 &= \frac{(-2)M}{N} + \frac{N}{N} \\
 &= 1 - \frac{2M}{N}
 \end{aligned}$$

Therefore, in the QFT case, we have $\Pr(y = 0)$ is very close to 1 and is given by

$$\Pr(y = 0) = 1 - \frac{4M}{N} + 4\frac{M^2}{N^2} = \left(1 - \frac{2M}{N}\right)^2$$

whereas in the Amplified-QFT case we have $\Pr(y = 0)$ is given by

$$\Pr(y = 0) = \cos^2 2k\theta$$

2.10.2 QFT Analysis: $Py = 0 \bmod N, y \neq 0$

We calculate the probability $\Pr(y)$ where $Py = 0 \bmod N, y \neq 0$.

Using the fact that

$$\sum_{z=0}^{N-1} \omega^{zy} = \frac{1 - \omega^{Ny}}{1 - \omega^y} = 0$$

we have

$$\begin{aligned}
Amp(y) &= \frac{-2}{N} \sum_{z \in A} \omega^{zy} + \frac{1}{N} \sum_{z=0}^{N-1} \omega^{zy} \\
&= \frac{-2}{N} \omega^{sy} \sum_{r=0}^{M-1} \omega^{rPy} \\
&= \frac{-2M}{N} \omega^{sy}
\end{aligned}$$

Therefore in the QFT case we have $\Pr(y)$ where $Py = 0 \pmod{N}, y \neq 0$ is given by

$$\Pr(y) = 4 \frac{M^2}{N^2}$$

which is small as $M \ll N$, whereas in the Amplified-QFT case we have $\Pr(y)$ is given by

$$\Pr(y) = \tan^2 \theta \sin^2 2k\theta$$

We can determine how the increase in amplitude varies with the number of iterations k of the Grover step in the Amplified-QFT by examining the ratio of the amplitudes of the Amplified-QFT case and QFT case. This ratio is given exactly by

$$\begin{aligned}
AmpRatio(y) &= \frac{\frac{(a_k - b_k)}{\sqrt{N}} \omega^{sy} M}{\frac{-2M}{N} \omega^{sy}} \\
&= \frac{(a_k - b_k)}{-2} \sqrt{N} \\
&= \frac{1}{-2} \left[\sqrt{\frac{N}{M}} \sin(2k+1)\theta - \sqrt{\frac{N}{N-M}} \cos(2k+1)\theta \right] \\
&= \frac{N}{-2M} \tan \theta \sin 2k\theta
\end{aligned}$$

We have the following for the probability ratio $\Pr Ratio(y)$, the increase in probability due to amplification

$$\Pr Ratio(y) = \frac{N^2 \tan^2 \theta \sin^2 2k\theta}{4M^2}$$

Using $k = \lfloor \frac{\pi}{4\theta} \rfloor$ and making use of

$$\frac{M}{N} \left(\frac{N}{N-M} \right) \geq \tan^2 \theta \sin^2 2k\theta \geq \frac{M}{N} \left(\frac{N}{N-M} \right) \left(\frac{N-2M}{N} \right)^2$$

we have the following inequality for the $\Pr Ratio(y)$:

$$\begin{aligned} \frac{N}{4M} \left(\frac{N}{N-M} \right) &\geq \Pr Ratio(y) \geq \frac{N}{4M} \left(\frac{N}{N-M} \right) \left(1 - \frac{2M}{N} \right)^2 \\ &\implies \Pr Ratio(y) \approx \frac{N}{4M} \end{aligned}$$

2.10.3 QFT Analysis: $Py \neq 0 \pmod N$

We calculate the probability $\Pr(y)$ in the case where $Py \neq 0 \pmod N$.

We have

$$\begin{aligned} Amp(y) &= \frac{-2}{N} \sum_{z \in A} \omega^{zy} + \frac{1}{N} \sum_{z=0}^{N-1} \omega^{zy} \\ &= \frac{-2}{N} w^{sy} \sum_{r=0}^{M-1} \omega^{rPy} \\ &= \frac{-2}{N} w^{sy} \left[\frac{1 - \omega^{MPy}}{1 - \omega^{Py}} \right] \\ &= \frac{-2}{N} w^{sy} \left[\frac{1 - \omega^{MPy}}{1 - \omega^{Py}} \right] \end{aligned}$$

Once again, making use of the following identity

$$|1 - e^{i\theta}|^2 = 4 \sin^2(\theta/2)$$

in the QFT case, we have $\Pr(y)$ where $Py \neq 0 \pmod N$ is given by

$$\Pr(y) = \frac{4}{N^2} \left[\frac{\sin^2(\pi MPy/N)}{\sin^2(\pi Py/N)} \right]$$

whereas in the Amplified-QFT case we have $\Pr(y)$ is given by

$$\Pr(y) = \frac{1}{M^2} \tan^2 \theta \sin^2 2k\theta \frac{\sin^2(\pi MPy/N)}{\sin^2(\pi Py/N)}$$

We note that

$$0 \leq \frac{\sin^2(\pi MPy/N)}{\sin^2(\pi Py/N)} \leq M^2$$

We notice that if in addition $MPy = 0 \bmod N$ then $\Pr(y) = 0$.

The ratio of the amplitudes of the Amplified-QFT case and QFT case is given exactly by

$$\begin{aligned} \text{AmpRatio}(y) &= \frac{\frac{(a_k - b_k)}{\sqrt{N}} \omega^{sy} \left[\frac{1 - \omega^{MPy}}{1 - \omega^{Py}} \right]}{\frac{-2}{N} w^{sy} \left[\frac{1 - \omega^{MPy}}{1 - \omega^{Py}} \right]} \\ &= \frac{(a_k - b_k)}{-2} \sqrt{N} \\ &= \frac{1}{-2} \left[\sqrt{\frac{N}{M}} \sin(2k+1)\theta - \sqrt{\frac{N}{N-M}} \cos(2k+1)\theta \right] \\ &= \frac{N}{-2M} \tan \theta \sin 2k\theta \end{aligned}$$

We note that this ratio is the same as in that given in the previous section and is independent of y . The variables in this ratio do not depend in anyway on the QFT.

We have the following for the probability ratio $\Pr \text{Ratio}(y)$, the increase in probability due to amplification

$$\Pr \text{Ratio}(y) = \frac{N^2 \tan^2 \theta \sin^2 2k\theta}{4M^2}$$

As in the previous section, we have the following inequality for the $\Pr \text{Ratio}(y)$, the increase in the probability due to amplification when $k = \lfloor \frac{\pi}{4\theta} \rfloor$ and making use of $\frac{M}{N}(\frac{N}{N-M}) \geq \tan^2 \theta \sin^2 2k\theta \geq \frac{M}{N}(\frac{N}{N-M})(\frac{N-2M}{N})^2$

$$\begin{aligned} \frac{N}{4M}(\frac{N}{N-M}) &\geq \Pr \text{Ratio}(y) \geq \frac{N}{4M}(\frac{N}{N-M})(1 - \frac{2M}{N})^2 \\ &\implies \Pr \text{Ratio}(y) \approx \frac{N}{4M} \end{aligned}$$

2.10.4 QFT Summary

The probability $\Pr(y)$ for the QFT is summarized in the following table and is given exactly by

$$\left\{ \begin{array}{ll} \left(1 - \frac{2M}{N}\right)^2 & \text{if } y = 0 \\ 4\frac{M^2}{N^2} & \text{if } Py = 0 \bmod N, y \neq 0 \\ \frac{4}{N^2} \frac{\sin^2(\pi MPy/N)}{\sin^2(\pi Py/N)} & \text{if } Py \neq 0 \bmod N \text{ and } MPy \neq 0 \bmod N \\ 0 & \text{if } Py \neq 0 \bmod N \text{ and } MPy = 0 \bmod N \end{array} \right\}$$

2.11 The QHS Algorithm - Detailed Analysis

In this section we examine the QHS algorithm in detail and produce the results for the probability of success that were summarized earlier in the paper. The QHS

algorithm is a two register algorithm as follows (see ref[13] for details). We begin with $|0\rangle|0\rangle$ where the first register is n qubits and the second register is 1 qubit and apply the Hadamard transform to the first register to get a uniform superposition state, followed by the unitary transformation for the Oracle f to get:

$$|\psi\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle |f(x)\rangle$$

Next we apply the QFT to the first register to get

$$\begin{aligned} |\psi\rangle &= \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} \omega^{xy} |y\rangle |f(x)\rangle \\ &= \sum_{y=0}^{N-1} \frac{1}{N} \sum_{x=0}^{N-1} \omega^{xy} |y\rangle |f(x)\rangle \\ &= \sum_{y=0}^{N-1} \frac{1}{N} |y\rangle \sum_{x=0}^{N-1} \omega^{xy} |f(x)\rangle \\ &= \sum_{y=0}^{N-1} \frac{||\Gamma(y)\rangle||}{N} |y\rangle \frac{|\Gamma(y)\rangle}{||\Gamma(y)\rangle||} \end{aligned}$$

where

$$\begin{aligned} |\Gamma(y)\rangle &= \sum_{x=0}^{N-1} \omega^{xy} |f(x)\rangle \\ &= \sum_{x \in A} \omega^{xy} |1\rangle + \sum_{x \notin A} \omega^{xy} |0\rangle \end{aligned}$$

and where

$$||\Gamma(y)\rangle||^2 = \left| \sum_{x \in A} \omega^{xy} \right|^2 + \left| \sum_{x \notin A} \omega^{xy} \right|^2$$

Next we make a measurement to get y and find that the probability of this measurement is

$$\Pr(y) = \frac{||\Gamma(y)\rangle||^2}{N^2}$$

$$= \frac{1}{N^2} \left| \sum_{x \in A} \omega^{xy} \right|^2 + \frac{1}{N^2} \left| \sum_{x \notin A} \omega^{xy} \right|^2$$

The state that we end up in is of the form

$$|\phi\rangle = |y\rangle \frac{|\Gamma(y)\rangle}{\| |\Gamma(y)\rangle \|}$$

We calculate the $\Pr(y)$ for the following cases:

- a) $y = 0$
- b) $Py = 0 \bmod N$ and $y \neq 0$
- c) $Py \neq 0 \bmod N$

2.11.1 QHS Analysis: $y = 0$

We calculate $\Pr(y = 0)$

We have

$$\begin{aligned} \Pr(y) &= \frac{1}{N^2} \left| \sum_{x \in A} \omega^{xy} \right|^2 + \frac{1}{N^2} \left| \sum_{x \notin A} \omega^{xy} \right|^2 \\ &= \frac{M^2}{N^2} + \frac{(N - M)^2}{N^2} = \frac{M^2 + N^2 - 2NM + M^2}{N^2} \\ &= 1 - \frac{2M(N - M)}{N^2} \end{aligned}$$

which is close to 1, whereas in the Amplified-QFT case we have $\Pr(y = 0)$ is given by

$$\Pr(y = 0) = \cos^2 2k\theta$$

2.11.2 QHS Analysis: $Py = 0 \bmod N, y \neq 0$

We calculate $\Pr(y)$ where $Py = 0 \bmod N, y \neq 0$.

We have

$$\begin{aligned}
\Pr(y) &= \frac{1}{N^2} \left| \sum_{x \in A} \omega^{xy} \right|^2 + \frac{1}{N^2} \left| \sum_{x \notin A} \omega^{xy} \right|^2 \\
&= \frac{1}{N^2} \left| \omega^{sy} \sum_{r=0}^{M-1} \omega^{rPy} \right|^2 + \frac{1}{N^2} \left| \sum_{x \notin A} \omega^{xy} \right|^2 \\
&= \frac{1}{N^2} \left| \omega^{sy} \sum_{r=0}^{M-1} \omega^{rPy} \right|^2 + \frac{1}{N^2} \left| -\omega^{sy} \sum_{r=0}^{M-1} \omega^{rPy} + \frac{1}{N} \sum_{x=0}^{N-1} \omega^{xy} \right|^2 \\
&= \frac{2M^2}{N^2}
\end{aligned}$$

which is small because $M \ll N$ and where we have used the fact that

$$\sum_{x=0}^{N-1} \omega^{xy} = 0$$

In the Amplified-QFT case we have $\Pr(y)$ is given by

$$\Pr(y) = \tan^2 \theta \sin^2 2k\theta$$

We have $\Pr \text{Ratio}(y) = \Pr(y)_{\text{Amplified-QFT}} / \Pr(y)_{\text{QHS}}$, the increase in the probability due to amplification is given by

$$\frac{N^2 \tan^2 \theta \sin^2 2k\theta}{2M^2}$$

We have the following inequality for the

$$\Pr \text{Ratio}(y) = \Pr(y)_{\text{Amplified-QFT}} / \Pr(y)_{\text{QHS}}$$

where $k = \lfloor \frac{\pi}{4\theta} \rfloor$ and making use of $\frac{M}{N}(\frac{N}{N-M}) \geq \tan^2 \theta \sin^2 2k\theta \geq \frac{M}{N}(\frac{N}{N-M})(\frac{N-2M}{N})^2$

$$\begin{aligned}
\frac{N}{2M}(\frac{N}{N-M}) &\geq \Pr \text{Ratio}(y) \geq \frac{N}{2M}(\frac{N}{N-M})(1 - \frac{2M}{N})^2 \\
&\implies \Pr \text{Ratio}(y) \approx \frac{N}{2M}
\end{aligned}$$

2.11.3 QHS Analysis: $Py \neq 0 \pmod N$

We calculate $\Pr(y)$ where $Py \neq 0 \pmod N$.

We have

$$\begin{aligned}
\Pr(y) &= \frac{1}{N^2} \left| \sum_{x \in A} \omega^{xy} \right|^2 + \frac{1}{N^2} \left| \sum_{x \notin A} \omega^{xy} \right|^2 \\
&= \frac{1}{N^2} \left| \omega^{sy} \sum_{r=0}^{M-1} \omega^{rPy} \right|^2 + \frac{1}{N^2} \left| \sum_{x \notin A} \omega^{xy} \right|^2 \\
&= \frac{1}{N^2} \left| \omega^{sy} \sum_{r=0}^{M-1} \omega^{rPy} \right|^2 + \frac{1}{N^2} \left| -\omega^{sy} \sum_{r=0}^{M-1} \omega^{rPy} + \frac{1}{N} \sum_{x=0}^{N-1} \omega^{xy} \right|^2 \\
&= \frac{1}{N^2} \left| \omega^{sy} \left[\frac{1 - \omega^{MPy}}{1 - \omega^{Py}} \right] \right|^2 + \frac{1}{N^2} \left| -\omega^{sy} \left[\frac{1 - \omega^{MPy}}{1 - \omega^{Py}} \right] \right|^2 \\
&= \frac{2}{N^2} \frac{\sin^2(\pi MPy/N)}{\sin^2(\pi Py/N)}
\end{aligned}$$

where we have used the fact that

$$\sum_{x=0}^{N-1} \omega^{xy} = 0$$

and that

$$|1 - e^{i\theta}|^2 = 4 \sin^2(\theta/2)$$

In the Amplified-QFT case we have $\Pr(y)$ is given by

$$\Pr(y) = \frac{1}{M^2} \tan^2 \theta \sin^2 2k\theta \frac{\sin^2(\pi MPy/N)}{\sin^2(\pi Py/N)}$$

We note that

$$0 \leq \frac{\sin^2(\pi MPy/N)}{\sin^2(\pi Py/N)} \leq M^2$$

We notice that if in addition $MPy = 0 \pmod N$ then $\Pr(y) = 0$.

We have the $\Pr \text{Ratio}(y) = \Pr(y)_{\text{Amplified-QFT}} / \Pr(y)_{\text{QHS}}$, the increase in the probability due to amplification is given by

$$\Pr \text{Ratio}(y) = \frac{N^2 \tan^2 \theta \sin^2 2k\theta}{2M^2}$$

We have the following inequality for the $\Pr \text{Ratio}(y)$ where $k = \lfloor \frac{\pi}{4\theta} \rfloor$ and making use of $\frac{M}{N}(\frac{N}{N-M}) \geq \tan^2 \theta \sin^2 2k\theta \geq \frac{M}{N}(\frac{N}{N-M})(\frac{N-2M}{N})^2$

$$\begin{aligned} \frac{N}{2M}(\frac{N}{N-M}) &\geq \Pr \text{Ratio}(y) \geq \frac{N}{2M}(\frac{N}{N-M})(1 - \frac{2M}{N})^2 \\ &\implies \Pr \text{Ratio}(y) \approx \frac{N}{2M} \end{aligned}$$

2.11.4 QHS Summary

We summarize the results for the QHS case. The $\Pr(y)$ is given exactly by:

$$\left\{ \begin{array}{ll} 1 - \frac{2M(N-M)}{N^2} & \text{if } y = 0 \\ \frac{2M^2}{N^2} & \text{if } Py = 0 \bmod N, y \neq 0 \\ \frac{2}{N^2} \frac{\sin^2(\pi MPy/N)}{\sin^2(\pi Py/N)} & \text{if } Py \neq 0 \bmod N \text{ and } MPy \neq 0 \bmod N \\ 0 & \text{if } Py \neq 0 \bmod N \text{ and } MPy = 0 \bmod N \end{array} \right\}$$

2.12 Recovering the Period P and the Offset s

As in Shor's algorithm, we use the continued fraction expansion of y/N to find the period P , where y is a measured value such that y/N is close to d/P and $(d, P) = 1$. See ref[2] and ref[3] for details which we provide below.

Let $\{a\}_N$ be the residue of $a \bmod N$ of smallest magnitude such that $-N/2 < \{a\}_N < N/2$. Let $S_N = \{0, 1, \dots, N-1\}$, $S_P = \{d \in S_N : 0 \leq d < P\}$ and $Y = \{y \in S_N : |\{Py\}_N| \leq P/2\}$. Then the map $Y \rightarrow S_P$ given by $y \rightarrow d = d(y) = \text{round}(Py/N)$ with inverse $y = y(d) = \text{round}(Nd/P)$ is a bijection and $\{Py\}_N = Py - Nd(y)$. In addition the following two sets are in 1-1 correspondence $\{y/N : y \in Y\}$ and $\{d/P : 0 \leq d < P\}$.

We make use of the following theorem from the theory of continued fractions ref[5] (Theorem 184 p.153):

Theorem 1. *Let x be a real number and let a and b be integers with $b > 0$. If $|x - \frac{a}{b}| \leq \frac{1}{2b^2}$ then the rational a/b is a convergent of the continued fraction expansion of x .*

Corollary 2. *If $P^2 \leq N$ and $|\{Py\}_N| \leq \frac{P}{2}$ then $d(y)/P$ is a convergent of the continued fraction expansion of y/N .*

Proof. Since $\{Py\}_N = Py - Nd(y)$ we have $|Py - Nd(y)| \leq \frac{P}{2}$ or $|\frac{y}{N} - \frac{d(y)}{P}| \leq \frac{1}{2N} \leq \frac{1}{2P^2}$ and we can apply Theorem 1 so that d/P is a convergent of the continued fraction expansion of y/N . \square

Since we know y and N we can find the continued fraction expansion of y/N .

However we also need that $(d, P) = 1$ in order that d/P is a convergent and enabling us to read off P directly. The probability that $(d, P) = 1$ is $\varphi(P)/P$ where $\varphi(P)$ is Euler's totient function. If P is prime we get $(d, P) = 1$ trivially.

By making use of the following Theorem it can be shown that

$$\frac{\varphi(P)}{P} \geq \frac{e^{-\gamma} - \epsilon(P)}{\ln 2} \frac{1}{\ln \ln N}$$

where $\epsilon(P)$ is a monotone decreasing sequence converging to zero.

Theorem 3. $\liminf \frac{\varphi(N)}{N/\ln \ln N} = e^{-\gamma}$

where $\gamma = 0.57721566$ is Euler's constant and where $e^{-\gamma} = 0.5614594836$.

This may cause us to repeat the experiment $\Omega(\frac{1}{\ln \ln N})$ times in order to get $(d, P) = 1$.

We note that we needed to add a condition on the period P that $P^2 \leq N$ or $P \leq \sqrt{N}$ in order for the proof of the corollary to work.

2.12.1 Testing if $P_1 = P$ when s is known or is 0

We can easily test if $s = 0$ by checking to see if $f(0) = 1$.

Now given a putative value of the period P_1 and a known offset or shift s , how can we test whether $P_1 = P$?

Assuming we have access to the Oracle to test individual values, we can confirm $f(s) = 1$ since s is known. We will show that if $f(s+P_1) = 1$ and $f(s+(M-1)P_1) = 1$ then $P_1 = P$.

Case 1: If $P_1 > P$ then $s + (M-1)P_1 > s + (M-1)P$. But $s + (M-1)P$

is the largest index x such that $f(x) = 1$. Therefore if $P_1 > P$ we must have $f(s + (M - 1)P_1) = 0$.

Case 2: If $0 < P_1 < P$ then $s < s + P_1 < s + P$ but between s and P there are no other values x such that $f(x) = 1$. Therefore if $0 < P_1 < P$ we must have $f(s + P_1) = 0$.

Therefore if $f(s) = 1, f(s + P_1) = 1$ and $f(s + (M - 1)P_1) = 1$ we must have $P_1 = P$.

2.12.2 Testing if $(s_1, P_1) = (s, P)$ when s is from a small known set and $s \neq 0$

If we assume s is unknown and $s \neq 0$ but is from a small known set of possible values such that we can exhaust over this set on a classical computer and we are given a putative value of the period P_1 , how can we test whether a pair of values (s_1, P_1) is the correct pair (s, P) ?

We need only test whether $f(s_1) = 1, f(s_1 + P_1) = 1$ and $f(s_1 + (M - 1)P_1) = 1$ where M is assumed known.

Case 1: If $s_1 < s$ then $f(s_1) = 0$ since s is the smallest index x with $f(x) = 1$.

Case 2: If $s_1 > s$ and $f(s_1) = 1$ then $s_1 = s + rP$ with $r > 0$. If $f(s_1 + P_1) = 1$ then $s_1 + P_1 = s + tP = s_1 + (t - r)P$ with $t > r > 0$. Hence $P_1 = (t - r)P > 0$. If $f(s_1 + (M - 1)P_1) = 1$ then $s_1 + (M - 1)P_1 = s + rP + (M - 1)(t - r)P > s + (M - 1)P$ which is the largest index x with $f(x) = 1$. Therefore $f(s_1 + (M - 1)P_1) = 0$.

Hence if $f(s_1) = 1, f(s_1 + P_1) = 1$ and $f(s_1 + (M - 1)P_1) = 1$ we must have

$s_1 = s$ and then by following the case when s is known we must also have $P_1 = P$.

Therefore if one or more of the values $f(s_1)$, $f(s_1 + P_1)$, $f(s_1 + (M - 1)P_1)$ is zero, either s_1 or P_1 is wrong. For a given P_1 we must exhaust over all possible values of s before we can be sure that $P_1 \neq P$. For in the case that $P_1 \neq P$, we will have for every possible s_1 that at least one of the values $f(s_1)$, $f(s_1 + P_1)$, $f(s_1 + (M - 1)P_1)$ is zero. In such a case we must try another putative P_1 .

2.12.3 Finding $s \neq 0$ using a Quantum Computer

We can assume $s \neq 0$ as the case $s = 0$ is trivial and was considered above. Let $s = \alpha + \beta P$ where $\alpha = s \bmod P$ so that $0 \leq \alpha \leq P - 1$ and $0 \leq \alpha + \beta P + (M - 1)P \leq N - 1$.

We assume we are given the correct value of P . If P is wrong, it will be detected in the algorithm.

Step 1:

We create an initial superposition on N values

$$|\psi_1\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle$$

and apply the Oracle f and put this into the amplitude. We then apply Grover without measurement to amplify the amplitudes and we have the following state

$$|\psi_1\rangle = a_k \sum_{x \in A} |x\rangle + b_k \sum_{x \notin A} |x\rangle$$

where

$$a_k = \frac{1}{\sqrt{M}} \sin(2k+1)\theta, b_k = \frac{1}{\sqrt{N-M}} \cos(2k+1)\theta$$

are the appropriate amplitudes of the states and where

$$\sin \theta = \sqrt{M/N}, \cos \theta = \sqrt{1 - M/N}$$

Next we measure the register and with probability exceeding $1 - M/N$ we will measure a value $x_1 \in A$ where $x_1 = s + r_1 P$ with $0 \leq r_1 \leq M-1$. Note that the total probability of the set A is given by

$$\begin{aligned} \Pr(x \in A) &= M \left(\frac{1}{\sqrt{M}} \sin(2k+1)\theta \right)^2 = \sin^2(2k+1)\theta = 1 - \cos^2(2k+1)\theta \\ \implies \Pr(x \in A) &= \sin^2(2k+1)\theta \geq 1 - \frac{M}{N} \end{aligned}$$

Now using our measured value $x_1 = s + r_1 P$ with $0 \leq r_1 \leq M-1$ we check that $f(x_1) = 1$ and $f(x_1 - P) = 1$. If $f(x_1 - P) = 0$ then either the value of P we are using is wrong or we have $r_1 = 0$ and $x_1 = s$. If we test $f(s) = 1$, $f(s + P) = 1$ and $f(s + (M-1)P) = 1$ then we have the correct P and s otherwise P is wrong. So assuming $f(x_1 - P) = 1$ we must have either the correct P or a multiple of P . We can use the procedure in Step 2 or Step 2' to find s . The method in Step 2 uses the Exact Quantum Counting algorithm to find s (See ref[11] for details). The method in Step 2' uses a method of decreasing sequence of measurements to find s .

Step 2 (using the Exact Quantum Counting algorithm):

Let T be such that $T \geq M$ is the smallest power of 2 greater than M . We form a superposition

$$|\varphi_1\rangle = \frac{1}{\sqrt{T}} \sum_{x=0}^{T-1} |x\rangle |0\rangle$$

and apply the function $g(x) = \text{Max}(0, x_1 - (x + 1)P)$ where $x_1 = s + r_1P$ is our measured value, with $0 \leq r_1 \leq M - 1$ and put the values of $g(x)$ into the second register to get

$$|\varphi_2\rangle = \frac{1}{\sqrt{T}} \sum_{x=0}^{T-1} |x\rangle |g(x)\rangle$$

Notice that as x increases from 0, $g(x)$ is a decreasing sequence $s + rP$ with $r = (r_1 - x - 1)$. When $g(x)$ dips below 0 we set $g(x) = 0$ to ensure $g(x) \geq 0$. Now we apply f to $g(x)$ and put the results into the amplitude to get

$$|\varphi_3\rangle = \frac{1}{\sqrt{T}} \sum_{x=0}^{T-1} (-1)^{f(g(x))} |x\rangle |g(x)\rangle$$

Notice that $f(g(x)) = 1$ when $s \leq g(x) < s + r_1P$ and is 0 elsewhere. We apply the exact quantum counting algorithm which determines how many values $f(g(x)) = 1$. Let this total be R . If P is correct we expect $R = r_1$ and we can determine $s = x_1 - RP = s + r_1P - RP$. We can then test if we have the correct pair of values s, P by testing whether $f(s) = 1$, $f(s + P) = 1$ and $f(s + (M - 1)P) = 1$. If this test fails then P must be an incorrect value and we must repeat the period finding algorithm.

We use Theorem 8.3.4 of ref[11]: The Exact Quantum Counting algorithm requires an expected number of applications of U_f in $O(\sqrt{(R + 1)(T - R + 1)})$ and outputs the correct value R with probability at least $2/3$.

Step 2' (decreasing sequence of measurements method):

Let T be such that $T \geq M$ is the smallest power of 2 greater than M . We form a superposition

$$|\varphi_1\rangle = \frac{1}{\sqrt{T}} \sum_{x=0}^{T-1} |x\rangle |0\rangle$$

and apply the function $g(x) = \text{Max}(0, x_1 - (x+1)P)$ where $x_1 = s + r_1P$ with $0 \leq r_1 \leq M-1$ and put these values into the second register to get

$$|\varphi_2\rangle = \frac{1}{\sqrt{T}} \sum_{x=0}^{T-1} |x\rangle |g(x)\rangle$$

Notice that as x increases from 0, $g(x)$ is a decreasing sequence $s + rP$ with $r = (r_1 - x - 1)$. When $g(x)$ dips below 0 we set $g(x) = 0$ to ensure $g(x) \geq 0$. Now we apply f to $g(x)$ and put the results into the third register and then into the amplitude.

$$|\varphi_3\rangle = \frac{1}{\sqrt{T}} \sum_{x=0}^{T-1} (-1)^{f(g(x))} |x\rangle |g(x)\rangle$$

Notice that $f(g(x)) = 1$ when $s \leq g(x) < s + r_1P$ and is 0 elsewhere.

We then run Grover without measurement to amplify the amplitudes and measure the second register containing $g(x)$.

With probability close to 1 we will measure a new value $x_2 = s + r_2P$ with $0 \leq r_2 < r_1$. We test the values $f(x_2) = 1$ and $f(x_2 - P) = 1$. If $f(x_2 - P) = 0$ then either the value of P we are using is wrong or we have $r_2 = 0$ and $x_2 = s$. If we test $f(s) = 1$, $f(s + P) = 1$ and $f(s + (M-1)P) = 1$ then we have the

correct P and s otherwise P is wrong. So assuming $f(x_2 - P) = 1$ we must have either the correct P or a multiple of P . We repeat this algorithm and go to Step 2' replacing the value x_1 in the function $g(x)$ with x_2 etc. As we repeat the algorithm we will measure a decreasing sequence of values x_1, x_2, \dots that converges to s . This procedure will eventually terminate with the correct pair of values P and s or we will determine that we have been using an incorrect value of P and we must repeat the quantum algorithm for finding putative P and repeat the process.

How many times do we expect to repeat Step 2'? When we make our first measurement we expect $r_1 = M/2$. For our second measurement we expect $r_2 = r_1/2$ etc. Therefore we expect to repeat this algorithm $O(\ln_2(M))$ times.

2.13 Replacing the QFT With a General Unitary Transform U

In general, if we had any Oracle f which is 1 on a set of labels A and 0 elsewhere and we replaced the QFT in the Amplified-QFT algorithm with any unitary transform U which performs the following

$$|z\rangle \rightarrow \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} \alpha(y, z) |y\rangle$$

we can compute the $AmpRatio(y) = \frac{Amplified-Amplitude(U)}{Amplitude(U)}$ as follows.

As before, we have the following state after applying U_f :

$$|\psi\rangle = \frac{1}{\sqrt{N}} \left[(-2) \sum_{z \in A} |z\rangle + \sum_{z=0}^{N-1} |z\rangle \right]$$

Next we apply the general unitary transform U to obtain the state

$$U|\psi\rangle = \sum_{y=0}^{N-1} \left[\frac{(-2)}{N} \sum_{z \in A} \alpha(y, z) + \frac{1}{N} \sum_{z=0}^{N-1} \alpha(y, z) \right] |y\rangle$$

In the Amplified-U case we apply Grover without measurement followed by U we obtain the state

$$|\phi_k\rangle = \sum_{y=0}^{N-1} \left[\frac{(a_k - b_k)}{\sqrt{N}} \sum_{z \in A} \alpha(y, z) + \frac{b_k}{\sqrt{N}} \sum_{z=0}^{N-1} \alpha(y, z) \right] |y\rangle$$

If $\sum_{z=0}^{N-1} \alpha(y, z) = 0$ and $\sum_{z \in A} \alpha(y, z) \neq 0$ we get the same $AmpRatio(y)$ formula that we obtained when $U = QFT$

$$\begin{aligned} AmpRatio(y) &= \frac{\frac{(a_k - b_k)}{\sqrt{N}} \sum_{z \in A} \alpha(y, z) + \frac{b_k}{\sqrt{N}} \sum_{z=0}^{N-1} \alpha(y, z)}{\frac{(-2)}{N} \sum_{z \in A} \alpha(y, z) + \frac{1}{N} \sum_{z=0}^{N-1} \alpha(y, z)} \\ &= \frac{\frac{(a_k - b_k)}{\sqrt{N}} \sum_{z \in A} \alpha(y, z)}{\frac{(-2)}{N} \sum_{z \in A} \alpha(y, z)} \\ &= \frac{\frac{(a_k - b_k)}{\sqrt{N}}}{\frac{(-2)}{N}} \\ &= \frac{(a_k - b_k)}{-2} \sqrt{N} \\ &= \frac{1}{-2} \left[\sqrt{\frac{N}{M}} \sin(2k+1)\theta - \sqrt{\frac{N}{N-M}} \cos(2k+1)\theta \right] \\ &= \frac{N}{-2M} \tan \theta \sin 2k\theta \end{aligned}$$

This gives

$$Pr\ Ratio(y) = \frac{N^2}{4M^2} \tan^2 \theta \sin^2 2k\theta$$

As in the case when $U=QFT$, we have the following inequality for the $Pr\ Ratio(y)$

for a general U , the increase in the probability due to amplification when $k = \lfloor \frac{\pi}{4\theta} \rfloor$

and making use of $\frac{M}{N}(\frac{N}{N-M}) \geq \tan^2 \theta \sin^2 2k\theta \geq \frac{M}{N}(\frac{N}{N-M})(\frac{N-2M}{N})^2$

$$\begin{aligned}\frac{N}{4M}(\frac{N}{N-M}) &\geq \Pr \text{Ratio}(y) \geq \frac{N}{4M}(\frac{N}{N-M})(1 - \frac{2M}{N})^2 \\ \implies \Pr \text{Ratio}(y) &\approx \frac{N}{4M}\end{aligned}$$

2.14 General Amplification Procedure With General Oracle

In this section we consider the case of a general amplification procedure with a general oracle followed by a QFT. We produce a general upper bound on the probability of measuring an observed value y .

Let f be a general oracle which is 1 on a set of labels A and 0 elsewhere. We assume there is a general amplification procedure which is unknown, which produces the following general state:

$$|\psi\rangle = \sum_{z=0}^{N-1} \sqrt{p_z} |z\rangle$$

where p_z is a probability distribution produced by a general amplification procedure. In addition we assume that

$$p(A) = \sum_{z \in A} p_z = \alpha \simeq 1$$

and

$$p(\bar{A}) = \sum_{z \notin A} p_z = 1 - \alpha \simeq 0$$

Next we apply the QFT to the state $|\psi\rangle$ by performing the following transformation

$$|z\rangle \rightarrow \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} \omega^{zy} |y\rangle$$

which gives the state

$$|\varphi\rangle = \sum_{y=0}^{N-1} \frac{1}{\sqrt{N}} \left[\sum_{z \in A} \sqrt{p_z} \omega^{zy} + \sum_{z \notin A} \sqrt{p_z} \omega^{zy} \right] |y\rangle$$

Next we wish to compute an upper bound on $P(y)$.

$$\begin{aligned} \Pr(y) &= \left| \frac{1}{\sqrt{N}} \sum_{z \in A} \sqrt{p_z} \omega^{zy} + \frac{1}{\sqrt{N}} \sum_{z \notin A} \sqrt{p_z} \omega^{zy} \right|^2 \\ &\leq \left| \frac{1}{\sqrt{N}} \sqrt{\left(\sum_{z \in A} p_z \right) \left(\sum_{z \in A} |\omega^{zy}|^2 \right)} + \frac{1}{\sqrt{N}} \sqrt{\left(\sum_{z \notin A} p_z \right) \left(\sum_{z \notin A} |\omega^{zy}|^2 \right)} \right|^2 \end{aligned}$$

by the Cauchy-Schwarz inequality

$$= \left(\sqrt{\alpha \frac{M}{N}} + \sqrt{(1-\alpha)(1-\frac{M}{N})} \right)^2$$

We see that in the specific case where the amplification procedure is perfect and $\alpha = 1$ the upper bound on $\Pr(y)$ is $\frac{M}{N}$. and otherwise, the upper bound on $\Pr(y)$ is close to $\frac{M}{N}$.

Next we generalize this further to the case where we have a general unitary transform U with entries $\frac{1}{\sqrt{N}} \alpha(y, z)$ such that $|\alpha(y, z)|^2 = 1$ for every y and z .

Let f be a general oracle which is 1 on a set of labels A and 0 elsewhere.

As before, we assume there is a general amplification procedure which is unknown, which produces the following general state:

$$|\psi\rangle = \sum_{x=0}^{N-1} \sqrt{p_x} |x\rangle$$

where p_x is a probability distribution produced by a general amplification procedure. In addition we assume that

$$p(A) = \sum_{z \in A} p_z = \alpha \simeq 1$$

and

$$p(\bar{A}) = \sum_{z \notin A} p_z = 1 - \alpha \simeq 0$$

Next we apply U to the state $|\psi\rangle$ by performing the following transformation

$$|z\rangle \rightarrow \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} \alpha(y, z) |y\rangle$$

which gives the state

$$|\varphi\rangle = \sum_{y=0}^{N-1} \frac{1}{\sqrt{N}} \left[\sum_{z \in A} \sqrt{p_z} \alpha(y, z) + \sum_{z \notin A} \sqrt{p_z} \alpha(y, z) \right] |y\rangle$$

Next we wish to compute an upper bound on $P(y)$.

$$\begin{aligned} \Pr(y) &= \left| \frac{1}{\sqrt{N}} \sum_{z \in A} \sqrt{p_z} \alpha(y, z) + \frac{1}{\sqrt{N}} \sum_{z \notin A} \sqrt{p_z} \alpha(y, z) \right|^2 \\ &\leq \left| \frac{1}{\sqrt{N}} \sqrt{\left(\sum_{z \in A} p_z \right) \left(\sum_{z \in A} |\alpha(y, z)|^2 \right)} + \frac{1}{\sqrt{N}} \sqrt{\left(\sum_{z \notin A} p_z \right) \left(\sum_{z \notin A} |\alpha(y, z)|^2 \right)} \right|^2 \end{aligned}$$

by the Cauchy-Schwarz inequality

$$= \left(\sqrt{\alpha \frac{M}{N}} + \sqrt{(1-\alpha)(1-\frac{M}{N})} \right)^2$$

Chapter 3: The Amplified Quantum Fourier Transform - With Error Stream

3.1 Introduction

In this paper, we generalize the results of the previous chapter ref[14] and show how to use the **Amplified-QFT algorithm** to solve the following problem:

The Local Period Finding Problem, with Error Stream: Let $\mathcal{L} = \{0, 1, \dots, N-1\}$ be a set of N labels, and let A be a periodic subset of M labels of period P , i.e., a subset of the form

$$A = \{j : j = s + rP, r = 0, 1, \dots, M-1\} ,$$

where $P \leq \sqrt{N}$ and $M \ll N$. Given a binary oracle

$$h : \mathcal{L} \longrightarrow \{0, 1\}$$

such that $h(x) = f(x) + g(x)$ where $+$ is the XOR operation and

$$f, g : \mathcal{L} \longrightarrow \{0, 1\}$$

and where $f(x) = 1$ on A and 0 elsewhere and $g(x)$ is an Error Stream which outputs a 1 with Bernoulli probability p and outputs a 0 with probability $q = 1 - p$. Let

$G = \{x|g(x) = 1\}$ with $|G| = L$ and let $C = A \cup G$ and let $T = L + M$, with $|C| = T$. We assume T is known because if it is unknown, we can find it using the quantum counting algorithm. We further assume that $A \cap G = \emptyset$ and note that $E[L] = Np$ and $Var[L] = Npq$.

The Amplified-QFT algorithm which solves this problem consists of three steps. **Step 1:** Apply Grover's algorithm without measurement to amplify the amplitudes of the T labels of the set C . **Step 2:** Apply the QFT to the resulting state. **Step 3:** Measurement.

We compare the probabilities of success of three algorithms that can be used to recover the period P : (1) Amplified-QFT (2) QFT and (3) QHS algorithms. Let the set $S_{ALG} = \{y : |\frac{y}{N} - \frac{d}{P}| \leq \frac{1}{2P^2}, (d, P) = 1\}$ be the set of "successful" y 's. That is S_{ALG} consists of those y 's which can be measured after applying one of the three algorithms denoted by ALG and from which the period P can be recovered by the method of continued fractions. We show

$$\frac{N}{4T}(\frac{N}{N-T}) \geq \frac{\Pr(S_{Amplified-QFT})}{\Pr(S_{QFT})} \geq \frac{N}{4T}(\frac{N}{N-T})(1 - \frac{2T}{N})^2$$

and

$$\frac{N}{2T}(\frac{N}{N-T}) \geq \frac{\Pr(S_{Amplified-QFT})}{\Pr(S_{QHS})} \geq \frac{N}{2T}(\frac{N}{N-T})(1 - \frac{2T}{N})^2$$

In the tables below, we summarize our results, comparing the probability of measuring a y in the final state arrived at after applying one of the three algorithms- Amplified-QFT, QFT and QHS, where $\sin \theta = \sqrt{T/N}$ and $k = \lfloor \frac{\pi}{4\theta} \rfloor$:

We compare each of the algorithms under the following four conditions on the

observation y :

Case A : $y = 0$

Case B : $Py = 0 \bmod N, y \neq 0$

Case C : $Py \neq 0 \bmod N$ and $MPy \neq 0 \bmod N$

Case D : $Py \neq 0 \bmod N$ and $MPy = 0 \bmod N$

Case 1 (Amplified-QFT):

The probability $\Pr(y)$ is given exactly by

$$\left\{ \begin{array}{l} \text{Case A: } \cos^2 2k\theta \\ \text{Case B: } \tan^2 \theta \sin^2 2k\theta \left| \frac{M}{T} \omega^{sy} + \frac{1}{T} \sum_{z \in G} \omega^{zy} \right|^2 \\ \text{Case C: } \tan^2 \theta \sin^2 2k\theta \left| \frac{1}{T} \omega^{sy} \left[\frac{1 - \omega^{MPy}}{1 - \omega^{Py}} \right] + \frac{1}{T} \sum_{z \in G} \omega^{zy} \right|^2 \\ \text{Case D: } \tan^2 \theta \sin^2 2k\theta \left| \frac{1}{T} \sum_{z \in G} \omega^{zy} \right|^2 \end{array} \right\}$$

Case 2 (QFT):

The probability $\Pr(y)$ is given exactly by

$$\left\{ \begin{array}{l} \text{Case A: } \left(1 - \frac{2T}{N}\right)^2 \\ \\ \text{Case B: } \frac{4}{N^2} \left| \omega^{sy} M + \sum_{z \in G} \omega^{zy} \right|^2 \\ \\ \text{Case C: } \frac{4}{N^2} \left| w^{sy} \left[\frac{1 - \omega^{MPy}}{1 - \omega^{Py}} \right] + \sum_{z \in G} \omega^{zy} \right|^2 \\ \\ \text{Case D: } \frac{4}{N^2} \left| \sum_{z \in G} \omega^{zy} \right|^2 \end{array} \right\}$$

Let y be fixed such that either Case B or Case C holds and define $\Pr \text{Ratio}(y) =$

$\Pr(y)_{\text{Amplified-QFT}} / \Pr(y)_{\text{QFT}}$ then we have the following

$$\begin{aligned} \frac{N}{4T} \left(\frac{N}{N-T} \right) &\geq \Pr \text{Ratio}(y) \geq \frac{N}{4T} \left(\frac{N}{N-T} \right) \left(1 - \frac{2T}{N} \right)^2 \\ &\implies \Pr \text{Ratio}(y) \approx \frac{N}{4T} \end{aligned}$$

Case 3 (QHS):

The probability $\Pr(y)$ is given exactly by

$$\left\{ \begin{array}{l} \text{Case A: } 1 - \frac{2T(N-T)}{N^2} \\ \\ \text{Case B: } \frac{2}{N^2} \left| \omega^{sy} M + \sum_{z \in G} \omega^{zy} \right|^2 \\ \\ \text{Case C: } \frac{2}{N^2} \left| \omega^{sy} \left[\frac{1 - \omega^{MPy}}{1 - \omega^{Py}} \right] + \sum_{z \in G} \omega^{zy} \right|^2 \\ \\ \text{Case D: } \frac{2}{N^2} \left| \sum_{z \in G} \omega^{zy} \right|^2 \end{array} \right\}$$

Let y be fixed such that either Case B or Case C holds and define $\text{Pr Ratio}(y) = \text{Pr}(y)_{\text{Amplified-QFT}} / \text{Pr}(y)_{QHS}$ then we have the following

$$\begin{aligned} \frac{N}{2T} \left(\frac{N}{N-T} \right) &\geq \text{Pr Ratio}(y) \geq \frac{N}{2T} \left(\frac{N}{N-T} \right) \left(1 - \frac{2T}{N} \right)^2 \\ &\implies \text{Pr Ratio}(y) \approx \frac{N}{2T} \end{aligned}$$

Let $S_{ALG} = \{y : |\frac{y}{N} - \frac{d}{P}| \leq \frac{1}{2P^2}, (d, P) = 1\}$ be the set of "successful" y 's. That is S_{ALG} consists of those y 's which can be measured after applying one of the three algorithms denoted by ALG and from which the period P can be recovered by the method of continued fractions. Note that the set S_{ALG} is the same for each algorithm. However the probability of this set varies with each algorithm. We can see from the following that given y_1 and y_2 , whose probability ratios satisfy the same inequality, we can add their probabilities to get a new ratio that satisfies the same inequality. In this way we can add probabilities over a set on the numerator

and denominator and maintain the inequality:

$$\begin{aligned} A &> \frac{P(y1)}{Q(y1)} > B \text{ and } A > \frac{P(y2)}{Q(y2)} > B \\ \implies A &> \frac{P(y1) + P(y2)}{Q(y1) + Q(y2)} > B \end{aligned}$$

We see from the cases given above that

$$\frac{N}{4T} \left(\frac{N}{N-T} \right) \geq \frac{\Pr(S_{\text{Amplified-QFT}})}{\Pr(S_{\text{QFT}})} \geq \frac{N}{4T} \left(\frac{N}{N-T} \right) \left(1 - \frac{2T}{N} \right)^2$$

where the difference between the upper bound and lower bound is exactly 1 and that

$$\frac{N}{2T} \left(\frac{N}{N-T} \right) \geq \frac{\Pr(S_{\text{Amplified-QFT}})}{\Pr(S_{\text{QHS}})} \geq \frac{N}{2T} \left(\frac{N}{N-T} \right) \left(1 - \frac{2T}{N} \right)^2$$

where the difference between the upper bound and lower bound is exactly 2.

This shows that the Amplified-QFT is approximately $\frac{N}{4T}$ times more successful than the QFT and $\frac{N}{2T}$ times more successful than the QHS when $T \ll N$. In addition it also shows that the QFT is 2 times more successful than the QHS in this problem. However, the success of the Amplified-QFT algorithms comes at an increase in work factor of $O(\sqrt{\frac{N}{T}})$. We note that in the case that P is a prime number that $(d, P) = 1$ is met trivially. However when P is composite the algorithms may need to be rerun several times until $(d, P) = 1$ is satisfied.

3.2 Comparison of Results Between $L=0$ and $L>0$

In this section we compare the probabilities of making a measurement between the two cases a) where there is no error stream and $L = 0$ and b) where the error

stream is present and $L > 0$.

We compare each of the algorithms under the following four conditions on the observation y :

$$\text{Case A : } y = 0$$

$$\text{Case B : } Py = 0 \bmod N, y \neq 0$$

$$\text{Case C : } Py \neq 0 \bmod N \text{ and } MPy \neq 0 \bmod N$$

$$\text{Case D : } Py \neq 0 \bmod N \text{ and } MPy = 0 \bmod N$$

1) Amplified-QFT case

The following are the probabilities of making a measurement y when $L = 0$:

$$\text{Here } k_1 = \left\lfloor \frac{\pi}{4 \sin^{-1}(\sqrt{M/N})} \right\rfloor \text{ and } \sin \theta_1 = \sqrt{M/N}$$

$$\left\{ \begin{array}{l} \text{Case A: } \cos^2 2k_1 \theta_1 \\ \\ \text{Case B: } \tan^2 \theta_1 \sin^2 2k_1 \theta_1 \\ \\ \text{Case C: } \frac{1}{M} \tan^2 \theta_1 \sin^2 2k_1 \theta_1 \frac{\sin^2(\pi MPy/N)}{\sin^2(\pi Py/N)} \\ \\ \text{Case D: } 0 \end{array} \right\}$$

The following are the probabilities of making a measurement y when $L > 0$

Here $k_2 = \left\lfloor \frac{\pi}{4 \sin^{-1}(\sqrt{T/N})} \right\rfloor$ and $\sin \theta_2 = \sqrt{T/N}$

$$\left\{ \begin{array}{l} \text{Case A: } \cos^2 2k_2\theta_2 \\ \text{Case B: } \tan^2 \theta_2 \sin^2 2k_2\theta_2 \left| \frac{M}{T}\omega^{sy} + \frac{1}{T} \sum_{z \in G} \omega^{zy} \right|^2 \\ \text{Case C: } \tan^2 \theta_2 \sin^2 2k_2\theta_2 \left| \frac{1}{T}\omega^{sy} \left[\frac{1-\omega^{MPy}}{1-\omega^{Py}} \right] + \frac{1}{T} \sum_{z \in G} \omega^{zy} \right|^2 \\ \text{Case D: } \tan^2 \theta_2 \sin^2 2k_2\theta_2 \left| \frac{1}{T} \sum_{z \in G} \omega^{zy} \right|^2 \end{array} \right\}$$

We notice that in cases B, C and D with $L > 0$ the probability of measuring y now depends on y whereas when $L = 0$ it does not. In addition in cases B, C and D with $L > 0$ the probability depends upon a sum over a random set G : $\frac{1}{T} \sum_{z \in G} \omega^{zy}$.

Notice that $T = L + M > M$ and $\sin \theta_2 = \sqrt{T/N} > \sin \theta_1 = \sqrt{M/N}$ and $\theta_2 > \theta_1$.

In the following theorems and corollaries we calculate the expected value and variance of

Case B:

$$\left| \frac{M}{T}\omega^{sy} + \frac{1}{T} \sum_{z \in G} \omega^{zy} \right|^2$$

Case C:

$$\left| \frac{1}{T}\omega^{sy} \left[\frac{1-\omega^{MPy}}{1-\omega^{Py}} \right] + \frac{1}{T} \sum_{z \in G} \omega^{zy} \right|^2$$

Case D:

$$\left| \frac{1}{T} \sum_{z \in G} \omega^{zy} \right|^2$$

The results are summarized in the tables below. Let $\varphi = 2\pi MP_y/N$ and let $\theta = 2\pi Py/N$.

Then the expected values are:

$$\left\{ \begin{array}{l} \text{Case B: } (M^2 + L)/(L + M)^2 \\ \text{Case C: } \left(\frac{\sin^2 \frac{\varphi}{2}}{\sin^2 \frac{\theta}{2}} + L \right) / (L + M)^2 \\ \text{Case D: } L/(L + M)^2 \end{array} \right\}$$

and the variances are:

$$\left\{ \begin{array}{l} \text{Case B: } (L^2 - L + 2M^2L)/(L + M)^4 \\ \text{Case C: } \left(L^2 - L + 2 \frac{\sin^2 \frac{\varphi}{2}}{\sin^2 \frac{\theta}{2}} L \right) / (L + M)^4 \\ \text{Case D: } (L^2 - L)/(L + M)^4 \end{array} \right\}$$

First we show

$$E \left| \sum_{z \in G} \omega^{zy} \right|^2 = L$$

where the sum is taken over L uniform random variables which take values in $\{0, 1, \dots, N - 1\}$ and the expectation is computed over all such possible sums.

Theorem 4. *Let $G = \{z_1, z_2, \dots, z_L\}$ be a set of L uniform random variables which take values in $\{0, 1, \dots, N - 1\}$. Consider the expected value of $\left| \sum_{z_j \in G} \omega^{z_j y} \right|^2$ where*

the expectation is taken over all N^L sums then

$$E_z \left| \sum_{z_j \in G} \omega^{z_j y} \right|^2 = \frac{1}{N^L} \sum_{G=\{z_1, z_2, \dots, z_L\}} \left| \sum_{z_j \in G} \omega^{z_j y} \right|^2 = L$$

Proof. Let $\omega^{zy} = \cos(\theta_z) + i \sin(\theta_z)$ where $\theta_z = 2\pi zy/N$ then

$$\begin{aligned} & E_z \left| \sum_{z \in G} \omega^{zy} \right|^2 \\ &= \frac{1}{N^L} \sum_{G=\{z_1, z_2, \dots, z_L\}} \left| \sum_{z_j \in G} \omega^{z_j y} \right|^2 \\ &= \frac{1}{N^L} \sum_{G=\{z_1, z_2, \dots, z_L\}} \left| \sum_{z_j \in G} \cos(\theta_{z_j}) + i \sin(\theta_{z_j}) \right|^2 \\ &= \frac{1}{N^L} \sum_{G=\{z_1, z_2, \dots, z_L\}} \left(\left(\sum_{z_j \in G} \cos(\theta_{z_j}) \right)^2 + \left(\sum_{z_j \in G} \sin(\theta_{z_j}) \right)^2 \right) \\ &= \frac{1}{N^L} \sum_{G=\{z_1, z_2, \dots, z_L\}} \left(\sum_{x_j \in G} \sum_{y_j \in G} \cos(\theta_{x_j}) \cos(\theta_{y_j}) + \sum_{x_j \in G} \sum_{y_j \in G} \sin(\theta_{x_j}) \sin(\theta_{y_j}) \right) \\ &= \frac{1}{N^L} \sum_{G=\{z_1, z_2, \dots, z_L\}} \sum_{z_j \in G} \cos^2(\theta_{z_j}) + \sin^2(\theta_{z_j}) + \text{other terms} \\ &= \frac{1}{N^L} \sum_{G=\{z_1, z_2, \dots, z_L\}} \sum_{z_j \in G} 1 \\ &= \frac{1}{N^L} \sum_{G=\{z_1, z_2, \dots, z_L\}} L \\ &= L \end{aligned}$$

where we have used the fact that

$$\frac{1}{N^L} \sum_{G=\{z_1, z_2, \dots, z_L\}} \sum_{x_j \in G} \sum_{y_j \in G} \cos(\theta_{x_j}) \cos(\theta_{y_j}) = 0$$

where we sum over the variables independently for both cosines. In addition

$$\frac{1}{N^L} \sum_{G=\{z_1, z_2, \dots, z_L\}} \sum_{x_j \in G} \sum_{y_j \in G} \sin(\theta_{x_j}) \sin(\theta_{y_j}) = 0$$

where we sum over the variables independently for each sin. Another way to see this is to consider the integral approximations of these sums:

$$\begin{aligned}
& \frac{1}{2\pi} \int_{\theta_1=0}^{\theta_1=2\pi} \frac{1}{2\pi} \int_{\theta_2=0}^{\theta_2=2\pi} \cos(\theta_1) \cos(\theta_2) d\theta_2 d\theta_1 \\
&= \frac{1}{2\pi} \int_{\theta_1=0}^{\theta_1=2\pi} \cos(\theta_1) \frac{1}{2\pi} \int_{\theta_2=0}^{\theta_2=2\pi} \cos(\theta_2) d\theta_2 d\theta_1 \\
&= \frac{1}{2\pi} \int_{\theta_1=0}^{\theta_1=2\pi} \cos(\theta_1) 0 d\theta_1 = 0
\end{aligned}$$

and

$$\begin{aligned}
& \frac{1}{2\pi} \int_{\theta_1=0}^{\theta_1=2\pi} \frac{1}{2\pi} \int_{\theta_2=0}^{\theta_2=2\pi} \sin(\theta_1) \sin(\theta_2) d\theta_2 d\theta_1 \\
&= \frac{1}{2\pi} \int_{\theta_1=0}^{\theta_1=2\pi} \sin(\theta_1) \frac{1}{2\pi} \int_{\theta_2=0}^{\theta_2=2\pi} \sin(\theta_2) d\theta_2 d\theta_1 \\
&= \frac{1}{2\pi} \int_{\theta_1=0}^{\theta_1=2\pi} \sin(\theta_1) 0 d\theta_1 = 0
\end{aligned}$$

□

Theorem 5. Let $G = \{z_1, z_2, \dots, z_L\}$ be a set of L uniform random variables which take values in $\{0, 1, \dots, N-1\}$. Consider the expected value of

$$\left| a\omega^{sy} + b \sum_{z_j \in G} \omega^{z_j y} \right|^2$$

where the expectation is taken over all N^L sums then

$$\begin{aligned}
& E_z \left| a\omega^{sy} + b \sum_{z_j \in G} \omega^{z_j y} \right|^2 \\
&= \frac{1}{N^L} \sum_{G=\{z_1, z_2, \dots, z_L\}} \left| a\omega^{sy} + b \sum_{z_j \in G} \omega^{z_j y} \right|^2 \\
&= a^2 + b^2 L
\end{aligned}$$

Proof. Let $\omega^{zy} = \cos(\theta_z) + i \sin(\theta_z)$ where $\theta_z = 2\pi zy/N$ and $\omega^{sy} = \cos(\varphi) + i \sin(\varphi)$

where $\varphi = 2\pi sy/N$ then

$$\begin{aligned}
& E_z \left| a\omega^{sy} + b \sum_{z_j \in G} \omega^{z_j y} \right|^2 \\
&= \frac{1}{N^L} \sum_{G=\{z_1, z_2, \dots, z_L\}} \left| a\omega^{sy} + b \sum_{z_j \in G} \omega^{z_j y} \right|^2 \\
&= \frac{1}{N^L} \sum_{G=\{z_1, z_2, \dots, z_L\}} \left| a \cos(\varphi) + ai \sin(\varphi) + b \sum_{z_j \in G} \cos(\theta_{z_j}) + i \sin(\theta_{z_j}) \right|^2 \\
&= \frac{1}{N^L} \sum_{G=\{z_1, z_2, \dots, z_L\}} (a \cos(\varphi) + b \sum_{z_j \in G} \cos(\theta_{z_j}))^2 + (a \sin(\varphi) + b \sum_{z_j \in G} \sin(\theta_{z_j}))^2 \\
&= \frac{1}{N^L} \sum_{G=\{z_1, z_2, \dots, z_L\}} (a \cos(\varphi) + \sum_{x_j \in G} b \cos(\theta_{x_j}))(a \cos(\varphi) + \sum_{y_j \in G} b \cos(\theta_{y_j})) \\
&\quad + (a \sin(\varphi) + b \sum_{x_j \in G} \sin(\theta_{x_j}))(a \sin(\varphi) + b \sum_{y_j \in G} \sin(\theta_{y_j})) \\
&= \frac{1}{N^L} \sum_{G=\{z_1, z_2, \dots, z_L\}} (a^2 \cos^2(\varphi) + b^2 \sum_{x_j \in G} \sum_{y_j \in G} \cos(\theta_{x_j}) \cos(\theta_{y_j}) + \\
&\quad 2ab \cos(\varphi) \sum_{y_j \in G} \cos(\theta_{y_j})) \\
&\quad + (a^2 \sin^2(\varphi) + b^2 \sum_{x_j \in G} \sum_{y_j \in G} \sin(\theta_{x_j}) \sin(\theta_{y_j}) + \\
&\quad 2ab \sin(\varphi) \sum_{y_j \in G} \sin(\theta_{y_j})) \\
&= \frac{1}{N^L} \sum_{G=\{z_1, z_2, \dots, z_L\}} (a^2 \cos^2(\varphi) + a^2 \sin^2(\varphi) + \\
&\quad b^2 \sum_{x_j \in G} \sum_{y_j \in G} \cos(\theta_{x_j}) \cos(\theta_{y_j}) + b^2 \sum_{x_j \in G} \sum_{y_j \in G} \sin(\theta_{x_j}) \sin(\theta_{y_j})) \\
&= \frac{1}{N^L} \sum_{G=\{z_1, z_2, \dots, z_L\}} (a^2 + b^2 \sum_{x_j \in G} \sum_{y_j \in G} (\cos(\theta_{x_j}) \cos(\theta_{y_j}) + \sin(\theta_{x_j}) \sin(\theta_{y_j}))) \\
&= a^2 + b^2 L
\end{aligned}$$

from the previous theorem.

□

Corollary 6. *Let $G = \{z_1, z_2, \dots, z_L\}$ be a set of L uniform random variables which take values in $\{0, 1, \dots, N-1\}$. Consider the expected value of $\left|\frac{1}{T} \sum_{z_j \in G} \omega^{z_j y}\right|^2$ and $\left|\frac{M}{T} \omega^{sy} + \frac{1}{T} \sum_{z_j \in G} \omega^{z_j y}\right|^2$ where the expectation is taken over all N^L sums then*

$$\begin{aligned} E_z \left| \frac{1}{T} \sum_{z_j \in G} \omega^{z_j y} \right|^2 \\ &= L/T^2 \\ &= L/(L+M)^2 \\ &\rightarrow 0 \text{ as } L \rightarrow \infty \end{aligned}$$

and

$$\begin{aligned} E_z \left| \frac{M}{T} \omega^{sy} + \frac{1}{T} \sum_{z_j \in G} \omega^{z_j y} \right|^2 \\ &= (M^2 + L)/T^2 \\ &= (M^2 + L)/(L+M)^2 \\ &\rightarrow 0 \text{ as } L \rightarrow \infty \end{aligned}$$

Theorem 7. *Let $G = \{z_1, z_2, \dots, z_L\}$ be a set of L uniform random variables which take values in $\{0, 1, \dots, N-1\}$. Consider the expected value of*

$$\left| a + ic + b \sum_{z_j \in G} \omega^{z_j y} \right|^2$$

where the expectation is taken over all N^L sums then

$$E_z \left| a + ic + b \sum_{z_j \in G} \omega^{z_j y} \right|^2$$

$$\begin{aligned}
&= \frac{1}{N^L} \sum_{G=\{z_1, z_2 \dots z_L\}} \left| a + ic + b \sum_{z_j \in G} \omega^{z_j y} \right|^2 \\
&= a^2 + c^2 + b^2 L
\end{aligned}$$

Proof.

$$\begin{aligned}
&E_z \left| a + ic + b \sum_{z_j \in G} \omega^{z_j y} \right|^2 \\
&= \frac{1}{N^L} \sum_{G=\{z_1, z_2 \dots z_L\}} \left| a + ic + b \sum_{z_j \in G} \omega^{z_j y} \right|^2 \\
&= \frac{1}{N^L} \sum_{G=\{z_1, z_2 \dots z_L\}} \left| a + ic + b \sum_{z_j \in G} \cos(\theta_{z_j}) + i \sin(\theta_{z_j}) \right|^2 \\
&= \frac{1}{N^L} \sum_{G=\{z_1, z_2 \dots z_L\}} (a + b \sum_{z_j \in G} \cos(\theta_{z_j}))^2 + (c + b \sum_{z_j \in G} \sin(\theta_{z_j}))^2 \\
&= \frac{1}{N^L} \sum_{G=\{z_1, z_2 \dots z_L\}} (a + \sum_{x_j \in G} b \cos(\theta_{x_j}))(a + \sum_{y_j \in G} b \cos(\theta_{y_j})) \\
&\quad + (c + b \sum_{x_j \in G} \sin(\theta_{x_j}))(c + b \sum_{y_j \in G} \sin(\theta_{y_j})) \\
&= \frac{1}{N^L} \sum_{G=\{z_1, z_2 \dots z_L\}} (a^2 + b^2 \sum_{x_j \in G} \sum_{y_j \in G} \cos(\theta_{x_j}) \cos(\theta_{y_j}) + \\
&\quad 2ab \sum_{y_j \in G} \cos(\theta_{y_j})) \\
&\quad + (c^2 + b^2 \sum_{x_j \in G} \sum_{y_j \in G} \sin(\theta_{x_j}) \sin(\theta_{y_j}) + \\
&\quad 2cb \sum_{y_j \in G} \sin(\theta_{y_j})) \\
&= \frac{1}{N^L} \sum_{G=\{z_1, z_2 \dots z_L\}} (a^2 + c^2 + \\
&\quad b^2 \sum_{x_j \in G} \sum_{y_j \in G} \cos(\theta_{x_j}) \cos(\theta_{y_j}) + b^2 \sum_{x_j \in G} \sum_{y_j \in G} \sin(\theta_{x_j}) \sin(\theta_{y_j}))
\end{aligned}$$

$$\begin{aligned}
&= \frac{1}{N^L} \sum_{G=\{z_1, z_2, \dots, z_L\}} (a^2 + b^2 \sum_{x_j \in G} \sum_{y_j \in G} (\cos(\theta_{x_j}) \cos(\theta_{y_j}) + \sin(\theta_{x_j}) \sin(\theta_{y_j}))) \\
&= a^2 + c^2 + b^2 L
\end{aligned}$$

from the previous theorem.

□

Corollary 8. *Let $\varphi = 2\pi MPy/N$ and let $\theta = 2\pi Py/N$ then*

$$\begin{aligned}
&E \left| \frac{1}{T} \omega^{sy} \left[\frac{1 - \omega^{MPy}}{1 - \omega^{Py}} \right] + \frac{1}{T} \sum_{z \in G} \omega^{zy} \right|^2 \\
&= \frac{1}{T^2} \frac{\sin^2 \frac{\varphi}{2}}{\sin^2 \frac{\theta}{2}} + \frac{1}{T^2} L \\
&\leq \frac{M^2 + L}{T^2} \\
&= \frac{M^2 + L}{(M + L)^2} \\
&\rightarrow 0 \text{ as } L \rightarrow \infty
\end{aligned}$$

Proof. Let $\varphi = 2\pi MPy/N$ and let $\theta = 2\pi Py/N$ then

$$\begin{aligned}
\frac{1 - \omega^{MPy}}{1 - \omega^{Py}} &= \frac{1 - \cos \varphi - i \sin \varphi}{1 - \cos \theta - i \sin \theta} \\
&= \frac{[(1 - \cos \varphi) - i \sin \varphi][(1 - \cos \theta) + i \sin \theta]}{[(1 - \cos \theta) - i \sin \theta][(1 - \cos \theta) + i \sin \theta]} \\
&= \frac{[2 \sin^2 \frac{\varphi}{2} - i \sin \varphi][2 \sin^2 \frac{\theta}{2} + i \sin \theta]}{2 - 2 \cos \theta} \\
&= \frac{4 \sin^2 \frac{\varphi}{2} \sin^2 \frac{\theta}{2} - i 2 \sin \varphi \sin^2 \frac{\theta}{2} + i 2 \sin \theta \sin^2 \frac{\varphi}{2} + \sin \varphi \sin \theta}{4 \sin^2 \frac{\theta}{2}} \\
&\quad 4 \sin^2 \frac{\varphi}{2} \sin^2 \frac{\theta}{2} - i 4 \sin \frac{\varphi}{2} \cos \frac{\varphi}{2} \sin^2 \frac{\theta}{2} + \\
&= \frac{i 4 \sin \frac{\theta}{2} \cos \frac{\theta}{2} \sin^2 \frac{\varphi}{2} + 4 \sin \frac{\theta}{2} \cos \frac{\theta}{2} \sin \frac{\varphi}{2} \cos \frac{\varphi}{2}}{4 \sin^2 \frac{\theta}{2}} \\
&= \frac{\sin \frac{\varphi}{2} \sin \frac{\theta}{2} \cos(\frac{\varphi}{2} - \frac{\theta}{2}) + i \sin \frac{\varphi}{2} \sin \frac{\theta}{2} \sin(\frac{\varphi}{2} - \frac{\theta}{2})}{\sin^2 \frac{\theta}{2}}
\end{aligned}$$

$$= \frac{\sin \frac{\varphi}{2} [\cos(\frac{\varphi}{2} - \frac{\theta}{2}) + i \sin(\frac{\varphi}{2} - \frac{\theta}{2})]}{\sin \frac{\theta}{2}}$$

Let $\lambda = 2\pi sy/N$ then

$$\begin{aligned} & \frac{1}{T} (\cos \lambda + i \sin \lambda) \frac{1 - \omega^{MPy}}{1 - \omega^{Py}} \\ &= \frac{1}{T} (\cos \lambda + i \sin \lambda) \frac{\sin \frac{\varphi}{2} [\cos(\frac{\varphi}{2} - \frac{\theta}{2}) + i \sin(\frac{\varphi}{2} - \frac{\theta}{2})]}{\sin \frac{\theta}{2}} \\ &= \frac{1}{T} \frac{\sin \frac{\varphi}{2} [\cos \lambda \cos(\frac{\varphi}{2} - \frac{\theta}{2}) - \sin \lambda \sin(\frac{\varphi}{2} - \frac{\theta}{2}) + i [\cos \lambda \sin(\frac{\varphi}{2} - \frac{\theta}{2}) + \sin \lambda \cos(\frac{\varphi}{2} - \frac{\theta}{2})]}{\sin \frac{\theta}{2}} \\ &= a + ic \end{aligned}$$

then

$$\begin{aligned} & a^2 + c^2 \\ &= \frac{1}{T^2} \frac{\sin^2 \frac{\varphi}{2}}{\sin^2 \frac{\theta}{2}} [\cos^2 \lambda + \sin^2 \lambda] \\ &= \frac{1}{T^2} \frac{\sin^2 \frac{\varphi}{2}}{\sin^2 \frac{\theta}{2}} \end{aligned}$$

□

Theorem 9. Let $G = \{z_1, z_2, \dots, z_L\}$ be a set of L uniform random variables which take values in $\{0, 1, \dots, N-1\}$. Consider the variance of $\left| \sum_{z_j \in G} \omega^{z_j y} \right|^2$ then

$$\begin{aligned} \text{Var} \left| \sum_{z_j \in G} \omega^{z_j y} \right|^2 &= \frac{1}{N^L} \sum_{G=\{z_1, z_2, \dots, z_L\}} \left| \sum_{z_j \in G} \omega^{z_j y} \right|^4 - L^2 \\ &= 2L^2 - L - L^2 \\ &= L^2 - L \end{aligned}$$

Proof. Note that

$$\text{Var}(X) = E(X^2) - (E(X))^2$$

Let $\omega^{zy} = \cos(\theta_z) + i \sin(\theta_z)$ where $\theta_z = 2\pi zy/N$ and consider

$$\begin{aligned}
& \frac{1}{N^L} \sum_{G=\{z_1, z_2, \dots, z_L\}} \left| \sum_{z_j \in G} \omega^{z_j y} \right|^4 \\
&= \frac{1}{N^L} \sum_{G=\{z_1, z_2, \dots, z_L\}} \left| \sum_{z_j \in G} \cos(\theta_{z_j}) + i \sin(\theta_{z_j}) \right|^4 \\
&= \frac{1}{N^L} \sum_{G=\{z_1, z_2, \dots, z_L\}} \left(\left(\sum_{z_j \in G} \cos(\theta_{z_j}) \right)^2 + \left(\sum_{z_j \in G} \sin(\theta_{z_j}) \right)^2 \right)^2 \\
&= \frac{1}{N^L} \sum_{G=\{z_1, z_2, \dots, z_L\}} \left(\sum_{x_j \in G} \sum_{y_j \in G} \cos(\theta_{x_j}) \cos(\theta_{y_j}) + \sum_{x_j \in G} \sum_{y_j \in G} \sin(\theta_{x_j}) \sin(\theta_{y_j}) \right)^2 \\
&= \frac{1}{N^L} \sum_{G=\{z_1, z_2, \dots, z_L\}} \left(\sum_{u_j \in G} \sum_{v_j \in G} \sum_{x_j \in G} \sum_{y_j \in G} \cos(\theta_{u_j}) \cos(\theta_{v_j}) \cos(\theta_{x_j}) \cos(\theta_{y_j}) + \right. \\
&\quad \left. 2 \sum_{u_j \in G} \sum_{v_j \in G} \sum_{x_j \in G} \sum_{y_j \in G} \cos(\theta_{u_j}) \cos(\theta_{v_j}) \sin(\theta_{x_j}) \sin(\theta_{y_j}) + \right. \\
&\quad \left. \sum_{u_j \in G} \sum_{v_j \in G} \sum_{x_j \in G} \sum_{y_j \in G} \sin(\theta_{u_j}) \sin(\theta_{v_j}) \sin(\theta_{x_j}) \sin(\theta_{y_j}) \right) \\
&= \frac{1}{N^L} \sum_{G=\{z_1, z_2, \dots, z_L\}} \left(\sum_{z_j \in G} \cos^4(\theta_{z_j}) + \right. \\
&\quad \left. \frac{1}{2} \binom{4}{2} \sum_{x_j \in G} \sum_{\substack{y_j \in G \\ x_j \neq y_j}} \cos^2(\theta_{x_j}) \cos^2(\theta_{y_j}) + \right. \\
&\quad \left. 2 \sum_{x_j \in G} \sum_{\substack{y_j \in G \\ x_j \neq y_j}} \cos^2(\theta_{x_j}) \sin^2(\theta_{y_j}) + \right. \\
&\quad \left. 2 \sum_{z_j \in G} \cos^2(\theta_{z_j}) \sin^2(\theta_{z_j}) + \right. \\
&\quad \left. \sum_{z_j \in G} \sin^4(\theta_{z_j}) + \right)
\end{aligned}$$

$$\begin{aligned}
& \frac{1}{2} \binom{4}{2} \sum_{x_j \in G} \sum_{\substack{y_j \in G \\ x_j \neq y_j}} \sin^2(\theta_{x_j}) \sin^2(\theta_{y_j}) \\
& + \text{other terms}) \\
& = 3L/8 + \frac{6}{2}L(L-1)/4 + 2L(L-1)/4 + 2L/8 + 3L/8 + \frac{6}{2}L(L-1)/4 \\
& = L + 2L(L-1) = 2L^2 - L
\end{aligned}$$

where we have used the fact that the sum over the *other terms* is 0, and we have approximated the averages by integrals

$$\frac{1}{2\pi} \int_{\theta=0}^{\theta=2\pi} \cos^2(\theta) d\theta = \frac{1}{2\pi} \int_{\theta=0}^{\theta=2\pi} \sin^2(\theta) d\theta = 1/2$$

$$\begin{aligned}
\frac{1}{2\pi} \int_{\theta=0}^{\theta=2\pi} \cos^4(\theta) d\theta &= \frac{1}{2\pi} \int_{\theta=0}^{\theta=2\pi} \sin^4(\theta) d\theta = 3/8 \\
\frac{1}{2\pi} \int_{\theta=0}^{\theta=2\pi} \cos^2(\theta) \sin^2(\theta) d\theta &= 1/8
\end{aligned}$$

□

Theorem 10. Let $G = \{z_1, z_2, \dots, z_L\}$ be a set of L uniform random variables which take values in $\{0, 1, \dots, N-1\}$. Consider the variance of $\left| a\omega^{sy} + b \sum_{z_j \in G} \omega^{z_j y} \right|^2$ then

$$\begin{aligned}
& \text{Var} \left| a\omega^{sy} + b \sum_{z_j \in G} \omega^{z_j y} \right|^2 \\
& = \frac{1}{N^L} \sum_{G=\{z_1, z_2, \dots, z_L\}} \left| a\omega^{sy} + b \sum_{z_j \in G} \omega^{z_j y} \right|^4 - (a^2 + b^2 L)^2 \\
& = a^4 + b^4(2L^2 - L) + 4a^2 b^2 L - (a^2 + b^2 L)^2 \\
& = a^4 + b^4(2L^2 - L) + 4a^2 b^2 L - a^4 - 2a^2 b^2 L - b^4 L^2 \\
& = b^4(L^2 - L) + 2a^2 b^2 L
\end{aligned}$$

Proof. Note that

$$\text{Var}(X) = E(X^2) - (E(X))^2$$

Let $\omega^{zy} = \cos(\theta_z) + i \sin(\theta_z)$ where $\theta_z = 2\pi zy/N$ and $\omega^{sy} = \cos(\varphi) + i \sin(\varphi)$ where $\varphi = 2\pi sy/N$ then

$$\begin{aligned}
& E \left| a\omega^{sy} + b \sum_{z_j \in G} \omega^{z_j y} \right|^4 \\
&= \frac{1}{N^L} \sum_{G=\{z_1, z_2, \dots, z_L\}} \left| a\omega^{sy} + b \sum_{z_j \in G} \omega^{z_j y} \right|^4 \\
&= \frac{1}{N^L} \sum_{G=\{z_1, z_2, \dots, z_L\}} \left| a(\cos(\varphi) + i \sin(\varphi)) + b \sum_{z_j \in G} \cos(\theta_{z_j}) + i \sin(\theta_{z_j}) \right|^4 \\
&= \frac{1}{N^L} \sum_{G=\{z_1, z_2, \dots, z_L\}} [(a \cos(\varphi) + b \sum_{z_j \in G} \cos(\theta_{z_j}))^2 + (a \sin(\varphi) + b \sum_{z_j \in G} \sin(\theta_{z_j}))^2]^2 \\
&= \frac{1}{N^L} \sum_{G=\{z_1, z_2, \dots, z_L\}} [(a \cos(\varphi) + b \sum_{x_j \in G} \cos(\theta_{x_j}))(a \cos(\varphi) + b \sum_{y_j \in G} \cos(\theta_{y_j})) + \\
&\quad (a \sin(\varphi) + b \sum_{x_j \in G} \sin(\theta_{x_j}))(a \sin(\varphi) + b \sum_{y_j \in G} \sin(\theta_{y_j}))]^2 \\
&= \frac{1}{N^L} \sum_{G=\{z_1, z_2, \dots, z_L\}} [a^2 \cos^2(\varphi) + b^2 \sum_{x_j \in G} \sum_{y_j \in G} \cos(\theta_{x_j}) \cos(\theta_{y_j}) + \\
&\quad 2ab \cos(\varphi) \sum_{x_j \in G} \cos(\theta_{x_j}) + a^2 \sin^2(\varphi) + b^2 \sum_{x_j \in G} \sum_{y_j \in G} \sin(\theta_{x_j}) \sin(\theta_{y_j}) + \\
&\quad 2ab \sin(\varphi) \sum_{x_j \in G} \sin(\theta_{x_j})]^2 \\
&= \frac{1}{N^L} \sum_{G=\{z_1, z_2, \dots, z_L\}} [a^2 + b^2 \sum_{x_j \in G} \sum_{y_j \in G} \cos(\theta_{x_j}) \cos(\theta_{y_j}) + \\
&\quad b^2 \sum_{x_j \in G} \sum_{y_j \in G} \sin(\theta_{x_j}) \sin(\theta_{y_j}) + 2ab \cos(\varphi) \sum_{x_j \in G} \cos(\theta_{x_j}) + \\
&\quad 2ab \sin(\varphi) \sum_{x_j \in G} \sin(\theta_{x_j})]^2
\end{aligned}$$

$$\begin{aligned}
&= \frac{1}{N^L} \sum_{G=\{z_1, z_2, \dots, z_L\}} [a^4 + b^4 \left(\sum_{x_j \in G} \sum_{y_j \in G} \cos(\theta_{x_j}) \cos(\theta_{y_j}) + \right. \\
&\quad \left. \sum_{x_j \in G} \sum_{y_j \in G} \sin(\theta_{x_j}) \sin(\theta_{y_j}) \right)^2 + 4a^2b^2 \cos^2(\varphi) \sum_{x_j \in G} \sum_{y_j \in G} \cos(\theta_{x_j}) \cos(\theta_{y_j}) + \\
&\quad 4a^2b^2 \sin^2(\varphi) \sum_{x_j \in G} \sum_{y_j \in G} \sin(\theta_{x_j}) \sin(\theta_{y_j}) + 2a^2b^2 \left(\sum_{x_j \in G} \sum_{y_j \in G} \cos(\theta_{x_j}) \cos(\theta_{y_j}) + \right. \\
&\quad \left. \sum_{x_j \in G} \sum_{y_j \in G} \sin(\theta_{x_j}) \sin(\theta_{y_j}) \right) + \text{other terms}] \\
&= a^4 + b^4(2L^2 - L) + 4a^2b^2 \cos^2(\varphi)L/2 + 4a^2b^2 \sin^2(\varphi)L/2 + 2a^2b^2L \\
&= a^4 + b^4(2L^2 - L) + 4a^2b^2L
\end{aligned}$$

Then

$$\begin{aligned}
\text{Var} \left| a\omega^{sy} + b \sum_{z_j \in G} \omega^{z_j y} \right|^2 &= E \left| a\omega^{sy} + b \sum_{z_j \in G} \omega^{z_j y} \right|^4 - (a^2 + b^2L)^2 \\
&= a^4 + b^4(2L^2 - L) + 4a^2b^2L - (a^2 + b^2L)^2 \\
&= a^4 + b^4(2L^2 - L) + 4a^2b^2L - a^4 - 2a^2b^2L - b^4L^2 \\
&= b^4(L^2 - L) + 2a^2b^2L
\end{aligned}$$

□

Corollary 11. *Let $G = \{z_1, z_2, \dots, z_L\}$ be a set of L uniform random variables which take values in $\{0, 1, \dots, N-1\}$. Consider the variance of*

$$\left| \frac{1}{T} \sum_{z_j \in G} \omega^{z_j y} \right|^2$$

and

$$\left| \frac{M}{T} \omega^{sy} + \frac{1}{T} \sum_{z_j \in G} \omega^{z_j y} \right|^2$$

then

$$\begin{aligned}
& \text{Var}_z \left| \frac{1}{T} \sum_{z_j \in G} \omega^{z_j y} \right|^2 \\
&= \frac{(L^2 - L)}{T^4} \\
&= \frac{(L^2 - L)}{(L + M)^4} \\
&\rightarrow 0 \text{ as } L \rightarrow \infty
\end{aligned}$$

and

$$\begin{aligned}
& \text{Var}_z \left| \frac{M}{T} \omega^{sy} + \frac{1}{T} \sum_{z_j \in G} \omega^{z_j y} \right|^2 \\
&= \frac{(L^2 - L)}{T^4} + \frac{2M^2 L}{T^4} \\
&= \frac{(L^2 - L) + 2M^2 L}{(L + M)^4} \\
&\rightarrow 0 \text{ as } L \rightarrow \infty
\end{aligned}$$

Theorem 12. Let $G = \{z_1, z_2, \dots, z_L\}$ be a set of L uniform random variables which take values in $\{0, 1, \dots, N-1\}$. Consider the variance of $\left| a + ic + b \sum_{z_j \in G} \omega^{z_j y} \right|^2$ then

$$\begin{aligned}
& \text{Var} \left| a + ic + b \sum_{z_j \in G} \omega^{z_j y} \right|^2 \\
&= \frac{1}{N^L} \sum_{G=\{z_1, z_2, \dots, z_L\}} \left| a + ic + b \sum_{z_j \in G} \omega^{z_j y} \right|^4 - (a^2 + c^2 + b^2 L)^2 \\
&= a^4 + c^4 + b^4(2L^2 - L) + 4(a^2 + c^2)b^2 L - (a^4 + c^4 + b^4 L^2 + 2(a^2 + c^2)b^2 L) \\
&= b^4(L^2 - L) + 2(a^2 + c^2)b^2 L
\end{aligned}$$

Proof. Let $\omega^{zy} = \cos(\theta_z) + i \sin(\theta_z)$ where $\theta_z = 2\pi zy/N$ and $\omega^{sy} = \cos(\varphi) + i \sin(\varphi)$

where $\varphi = 2\pi sy/N$ then

$$\begin{aligned}
& E \left| a + ic + b \sum_{z_j \in G} \omega^{z_j y} \right|^4 \\
&= \frac{1}{N^L} \sum_{G=\{z_1, z_2, \dots, z_L\}} \left| a + ic + b \sum_{z_j \in G} \omega^{z_j y} \right|^4 \\
&= \frac{1}{N^L} \sum_{G=\{z_1, z_2, \dots, z_L\}} \left| a + ic + b \sum_{z_j \in G} \cos(\theta_{z_j}) + i \sin(\theta_{z_j}) \right|^4 \\
&= \frac{1}{N^L} \sum_{G=\{z_1, z_2, \dots, z_L\}} [(a + b \sum_{z_j \in G} \cos(\theta_{z_j}))^2 + (c + b \sum_{z_j \in G} \sin(\theta_{z_j}))^2]^2 \\
&= \frac{1}{N^L} \sum_{G=\{z_1, z_2, \dots, z_L\}} [(a + b \sum_{x_j \in G} \cos(\theta_{x_j}))(a + b \sum_{y_j \in G} \cos(\theta_{y_j})) + \\
&\quad (c + b \sum_{x_j \in G} \sin(\theta_{x_j}))(c + b \sum_{y_j \in G} \sin(\theta_{y_j}))]^2 \\
&= \frac{1}{N^L} \sum_{G=\{z_1, z_2, \dots, z_L\}} [a^2 + b^2 \sum_{x_j \in G} \sum_{y_j \in G} \cos(\theta_{x_j}) \cos(\theta_{y_j}) + \\
&\quad 2ab \sum_{x_j \in G} \cos(\theta_{x_j}) + c^2 + b^2 \sum_{x_j \in G} \sum_{y_j \in G} \sin(\theta_{x_j}) \sin(\theta_{y_j}) + \\
&\quad 2cb \sum_{x_j \in G} \sin(\theta_{x_j})]^2 \\
&= \frac{1}{N^L} \sum_{G=\{z_1, z_2, \dots, z_L\}} [a^2 + c^2 + b^2 \sum_{x_j \in G} \sum_{y_j \in G} \cos(\theta_{x_j}) \cos(\theta_{y_j}) + \\
&\quad b^2 \sum_{x_j \in G} \sum_{y_j \in G} \sin(\theta_{x_j}) \sin(\theta_{y_j}) + 2ab \sum_{x_j \in G} \cos(\theta_{x_j}) + \\
&\quad 2cb \sum_{x_j \in G} \sin(\theta_{x_j})]^2 \\
&= \frac{1}{N^L} \sum_{G=\{z_1, z_2, \dots, z_L\}} [a^4 + c^4 + b^4 (\sum_{x_j \in G} \sum_{y_j \in G} \cos(\theta_{x_j}) \cos(\theta_{y_j}) + \\
&\quad \sum_{x_j \in G} \sum_{y_j \in G} \sin(\theta_{x_j}) \sin(\theta_{y_j}))^2 + 4a^2 b^2 \sum_{x_j \in G} \sum_{y_j \in G} \cos(\theta_{x_j}) \cos(\theta_{y_j}) + \\
&\quad 4a^2 c^2 \sum_{x_j \in G} \sum_{y_j \in G} \cos(\theta_{x_j}) \sin(\theta_{y_j}) + 4c^2 b^2 \sum_{x_j \in G} \sum_{y_j \in G} \sin(\theta_{x_j}) \sin(\theta_{y_j}) + \\
&\quad 4ab^3 \sum_{x_j \in G} \sum_{y_j \in G} \cos(\theta_{x_j}) \cos(\theta_{y_j}) \sin(\theta_{y_j}) + 4ab^3 \sum_{x_j \in G} \sum_{y_j \in G} \cos(\theta_{x_j}) \sin(\theta_{y_j}) \sin(\theta_{y_j}) + \\
&\quad 4cb^3 \sum_{x_j \in G} \sum_{y_j \in G} \sin(\theta_{x_j}) \sin(\theta_{y_j}) \cos(\theta_{y_j}) + 4cb^3 \sum_{x_j \in G} \sum_{y_j \in G} \sin(\theta_{x_j}) \sin(\theta_{y_j}) \sin(\theta_{y_j})]
\end{aligned}$$

$$\begin{aligned}
& 4c^2b^2 \sum_{x_j \in G} \sum_{y_j \in G} \sin(\theta_{x_j}) \sin(\theta_{y_j}) + 2(a^2 + c^2)b^2 \left(\sum_{x_j \in G} \sum_{y_j \in G} \cos(\theta_{x_j}) \cos(\theta_{y_j}) + \right. \\
& \left. \sum_{x_j \in G} \sum_{y_j \in G} \sin(\theta_{x_j}) \sin(\theta_{y_j}) \right) + otherterms] \\
& = a^4 + c^4 + b^4(2L^2 - L) + 4a^2b^2L/2 + 4c^2b^2L/2 + 2(a^2 + c^2)b^2L \\
& = a^4 + c^4 + b^4(2L^2 - L) + 4(a^2 + c^2)b^2L
\end{aligned}$$

□

Corollary 13. *Let $\varphi = 2\pi MPy/N$ and let $\theta = 2\pi Py/N$*

$$\begin{aligned}
& Var \left| \frac{1}{T} \omega^{sy} \left[\frac{1 - \omega^{MPy}}{1 - \omega^{Py}} \right] + \frac{1}{T} \sum_{z \in G} \omega^{zy} \right|^2 \\
& = \frac{1}{T^4} (L^2 - L) + \frac{2}{T^4} \frac{\sin^2 \frac{\varphi}{2}}{\sin^2 \frac{\theta}{2}} L \\
& \leq \frac{(L^2 - L + 2M^2L)}{(L + M)^4} \\
& \rightarrow 0 \text{ as } L \rightarrow \infty
\end{aligned}$$

Proof. Let $\varphi = 2\pi MPy/N$, let $\theta = 2\pi Py/N$ and let $\lambda = 2\pi sy/N$ then $b = \frac{1}{T}$ and

from and earlier result

$$\begin{aligned}
& a^2 + c^2 \\
& = \frac{1}{T^2} \frac{\sin^2 \frac{\varphi}{2}}{\sin^2 \frac{\theta}{2}} \cdot [\cos^2 \lambda + \sin^2 \lambda] \\
& = \frac{1}{T^2} \frac{\sin^2 \frac{\varphi}{2}}{\sin^2 \frac{\theta}{2}} \\
& \leq \frac{M^2}{T^2}
\end{aligned}$$

□

Next we show that as L increases the upperbound of the expected value of the probability in Cases B and C decreases to a minimum value.

Lemma 14. *Let $k = \left\lfloor \frac{\pi}{4 \sin^{-1}(\sqrt{T/N})} \right\rfloor$ and $\sin \theta = \sqrt{T/N}$ where $T = L + M$ then the upperbound of the expected value of the probability in Cases B and C decreases to a minimum value at $MinL$ given by*

$$MinL = -M^2 + \sqrt{M(M-1)(M(M-1) + N)}$$

Proof. The probability in case B is given by

$$\tan^2 \theta \sin^2 2k\theta \left| \frac{M}{T} \omega^{sy} + \frac{1}{T} \sum_{z_j \in G} \omega^{z_j y} \right|^2$$

This has expected value

$$\frac{M^2 + L}{(L + M)^2} \tan^2 \theta \sin^2 2k\theta$$

The probability in case C is given by

$$\tan^2 \theta \sin^2 2k\theta \left| \frac{1}{T} \omega^{sy} \left[\frac{1 - \omega^{MPy}}{1 - \omega^{Py}} \right] + \frac{1}{T} \sum_{z \in G} \omega^{zy} \right|^2$$

This has expected value

$$\begin{aligned} & \left(\frac{1}{T^2} \frac{\sin^2 \frac{\varphi}{2}}{\sin^2 \frac{\theta}{2}} + \frac{1}{T^2} L \right) \tan^2 \theta \sin^2 2k\theta \\ & \leq \frac{M^2 + L}{(M + L)^2} \tan^2 \theta \sin^2 2k\theta \end{aligned}$$

Therefore the expected value of the probability in case B dominates the expected value in case C. We have by a later lemma that

$$\frac{T}{N - T} \geq \tan^2 \theta \sin^2 2k\theta \geq \left(\frac{T}{N - T} \right) (1 - 2T/N)^2$$

Therefore we have

$$\begin{aligned} \left(\frac{L+M}{N-(L+M)}\right) \frac{M^2+L}{(L+M)^2} &\geq \frac{M^2+L}{(L+M)^2} \tan^2 \theta \sin^2 2k\theta \\ \frac{1}{N-(L+M)} \frac{M^2+L}{(L+M)} &\geq \frac{M^2+L}{(L+M)^2} \tan^2 \theta \sin^2 2k\theta \end{aligned}$$

The upperbound of the expected value of the probability in Case B. decreases to a minimum value of L . If we differentiate it and set it to zero we can find the value of L where it is a minimum. Consider

$$\begin{aligned} &\frac{d}{dL} \frac{1}{N-(L+M)} \frac{M^2+L}{(L+M)} \\ &= \frac{1}{(N-(L+M))^2} \frac{M^2+L}{(L+M)} + \frac{1}{(N-(L+M))(L+M)} \\ &\quad - \frac{M^2+L}{(N-(L+M))(L+M)^2} \\ &= \frac{L^2 + 2M^2L + M(2M^2 + N - M - NM)}{(N-(L+M))^2(L+M)^2} \text{ after some rearranging} \end{aligned}$$

Therefore $MinL$ is a solution to the quadratic equation

$$L^2 + 2M^2L + M(2M^2 + N - M - NM) = 0$$

This has solutions

$$\begin{aligned} MinL &= \frac{1}{2}(-2M^2 \pm \sqrt{4M^4 - 4M(2M^2 + N - M - NM)}) \\ &= -M^2 \pm \sqrt{M(M-1)(M(M-1) + N)} \end{aligned}$$

Therefore the upper bound of the expected value of the probability achieves its minimum at $MinL$ given by

$$MinL = -M^2 + \sqrt{M(M-1)(M(M-1) + N)}$$

□

This shows that as L increases on the interval $[0, MinL]$ and more errors are introduced, the expected value of the probability of measuring any given y decreases, making it harder to recover the period P . Note that $MinL$ need not be an integer.

We can rewrite the function in the proof as

$$\begin{aligned} f(L) &= \frac{L + M^2}{(N - (L + M))(L + M)} \\ &= \frac{A}{N - (L + M)} + \frac{B}{(L + M)} \end{aligned}$$

then we have

$$A(L + M) + B(N - (L + M)) = L + M^2 \text{ then}$$

$$A - B = 1 \text{ and}$$

$$AM + B(N - M) = M^2$$

Solving these equations yields

$$\begin{aligned} A &= 1 + \frac{M(M - 1)}{N} \\ B &= \frac{M(M - 1)}{N} \end{aligned}$$

The first term in $f(L)$

$$\frac{A}{N - (L + M)}$$

is an increasing function of L whereas the second term

$$\frac{B}{(L + M)}$$

is a decreasing function of L . Adding these together produces a function that has a minimum value.

3.3 The Three Step Amplified-QFT algorithm

In this section we provide the calculations for the probabilities of success for the Amplified-QFT algorithm.

Problem: We are given a binary valued Oracle $h(x)$ on N labels $\{0, 1, \dots, N-1\}$, where $N = 2^n$, which takes the value 1 on $C = A \cup G$ where A is a periodic set of M labels and G is the set where the Error Stream $g(x) = 1$. We wish to determine the period P with the smallest number of queries of the Oracle.

The Amplified-QFT algorithm is defined by the following three step procedure.

Step 1: Apply all of Grover's algorithm in its entirety except for the last measurement step to the starting state $|0\rangle$. The resulting state is given by $|\psi_k\rangle$ (ref[4], ref[7], ref[1]) where $k = \left\lfloor \frac{\pi}{4 \sin^{-1}(\sqrt{T/N})} \right\rfloor$:

$$|\psi_k\rangle = a_k \sum_{z \in C} |z\rangle + b_k \sum_{z \notin C} |z\rangle$$

where

$$a_k = \frac{1}{\sqrt{T}} \sin(2k+1)\theta, b_k = \frac{1}{\sqrt{N-T}} \cos(2k+1)\theta$$

are the appropriate amplitudes of the states and where

$$\sin \theta = \sqrt{T/N}, \cos \theta = \sqrt{1 - T/N}$$

Step 2: The QFT performs the following action

$$|z\rangle \rightarrow \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} e^{-2\pi i z y / N} |y\rangle$$

After the application of the QFT to the state $|\psi_k\rangle$, letting $\omega = e^{-2\pi i / N}$, we have

$$|\phi_k\rangle = \frac{a_k}{\sqrt{N}} \sum_{z \in C} \sum_{y=0}^{N-1} \omega^{zy} |y\rangle + \frac{b_k}{\sqrt{N}} \sum_{z \notin C} \sum_{y=0}^{N-1} \omega^{zy} |y\rangle$$

After interchanging the order of summation, we have

$$|\phi_k\rangle = \sum_{y=0}^{N-1} \left[\frac{a_k}{\sqrt{N}} \sum_{z \in C} \omega^{zy} + \frac{b_k}{\sqrt{N}} \sum_{z \notin C} \omega^{zy} \right] |y\rangle$$

Step 3: Measure with respect to the standard basis to yield a integer $y \in \{0, 1, \dots, N-1\}$ from which we can determine the period P using the continued fraction method.

3.4 Analysis of the Amplified-QFT Algorithm

We calculate the $\Pr(y)$ for the following cases:

- a) $y = 0$
- b) $Py = 0 \bmod N$ and $y \neq 0$
- c) $Py \neq 0 \bmod N$

The amplitude $\text{Amp}(y)$ of $|y\rangle$ is given by

$$\begin{aligned} \text{Amp}(y) &= \frac{a_k}{\sqrt{N}} \sum_{z \in C} \omega^{zy} + \frac{b_k}{\sqrt{N}} \sum_{z \notin C} \omega^{zy} \\ &= \frac{a_k}{\sqrt{N}} \sum_{z \in A} \omega^{zy} + \frac{a_k}{\sqrt{N}} \sum_{z \in G} \omega^{zy} + \frac{b_k}{\sqrt{N}} \sum_{z \notin C} \omega^{zy} \end{aligned}$$

$$\begin{aligned}
&= \frac{(a_k - b_k)}{\sqrt{N}} \left[\sum_{z \in A} \omega^{zy} + \sum_{z \in G} \omega^{zy} \right] + \frac{b_k}{\sqrt{N}} \sum_{z=0}^{N-1} \omega^{zy} \\
&= \frac{(a_k - b_k)}{\sqrt{N}} \left[\sum_{r=0}^{M-1} \omega^{(s+rP)y} + \sum_{z \in G} \omega^{zy} \right] + \frac{b_k}{\sqrt{N}} \sum_{z=0}^{N-1} \omega^{zy} \\
&= \frac{(a_k - b_k)}{\sqrt{N}} \left[\omega^{sy} \sum_{r=0}^{M-1} \omega^{rPy} + \sum_{z \in G} \omega^{zy} \right] + \frac{b_k}{\sqrt{N}} \sum_{z=0}^{N-1} \omega^{zy}
\end{aligned}$$

In the following we use the following four lemmas:

Lemma 15.

$$\sum_{z=0}^{N-1} \omega^{zy} = \frac{1 - \omega^{Ny}}{1 - \omega^y} = 0, w^y \neq 1$$

Lemma 16.

$$\frac{T}{\sqrt{N}}(a_k - b_k) = \tan \theta \sin 2k\theta$$

Proof.

$$\begin{aligned}
\frac{T}{\sqrt{N}}(a_k - b_k) &= \frac{T}{\sqrt{NT}} \sin(2k+1)\theta - \frac{T}{\sqrt{N(N-T)}} \cos(2k+1)\theta \\
&= \sqrt{\frac{T}{N}} (\sin(2k+1)\theta - \sqrt{\frac{T}{(N-T)}} \cos(2k+1)\theta) \\
&= \sqrt{\frac{T}{N}} (\sin(2k+1)\theta - \sqrt{\frac{T/N}{(1-T/N)}} \cos(2k+1)\theta) \\
&= \sqrt{\frac{T}{N}} (\sin(2k+1)\theta - \frac{\sin \theta}{\cos \theta} \cos(2k+1)\theta) \\
&= \tan \theta (\cos \theta \sin(2k+1)\theta - \sin \theta \cos(2k+1)\theta) \\
&= \tan \theta \sin 2k\theta
\end{aligned}$$

□

Lemma 17.

$$\frac{T}{N} \left(\frac{N}{N-T} \right) \geq \tan^2 \theta \sin^2 2k\theta \geq \frac{T}{N} \left(\frac{N}{N-T} \right) \left(1 - \frac{2T}{N} \right)^2$$

Proof. Using $k = \lfloor \frac{\pi}{4\theta} \rfloor \implies \frac{\pi}{4\theta} - 1 \leq k \leq \frac{\pi}{4\theta} \implies \frac{\pi}{2} - 2\theta \leq 2k\theta \leq \frac{\pi}{2} \implies \sin(\frac{\pi}{2} - 2\theta) \leq \sin 2k\theta \leq 1$ we have

$$\begin{aligned}
\frac{\sin^2 \theta}{\cos^2 \theta} &\geq \tan^2 \theta \sin^2 2k\theta \geq \tan^2 \theta \sin^2(\frac{\pi}{2} - 2\theta) \\
&\implies \frac{T}{N} \frac{1}{1 - \frac{T}{N}} \geq \tan^2 \theta \sin^2 2k\theta \geq \tan^2 \theta \sin^2(\frac{\pi}{2} - 2\theta) \\
&\implies \frac{T}{N} (\frac{N}{N-T}) \geq \tan^2 \theta \sin^2 2k\theta \geq \frac{\sin^2 \theta}{\cos^2 \theta} \cos^2 2\theta \\
&\implies \frac{T}{N} (\frac{N}{N-T}) \geq \tan^2 \theta \sin^2 2k\theta \geq \frac{\sin^2 \theta}{\cos^2 \theta} (2 \cos^2 \theta - 1)^2 \\
&\implies \frac{T}{N} (\frac{N}{N-T}) \geq \tan^2 \theta \sin^2 2k\theta \geq \frac{T}{N} (\frac{N}{N-T}) (1 - \frac{2T}{N})^2
\end{aligned}$$

□

Lemma 18. *If $Py \neq 0 \pmod N$ then*

$$\left| \frac{1 - \omega^{MPy}}{1 - \omega^{Py}} \right|^2 = \frac{\sin^2(\pi MPy/N)}{\sin^2(\pi Py/N)} \leq M^2$$

Proof. We use the following result

$$|1 - e^{i\theta}|^2 = 4 \sin^2(\theta/2)$$

□

3.4.1 Amplified-QFT Analysis: $y = 0$

We have

$$Amp(y) = \frac{a_k}{\sqrt{N}} \sum_{z \in C} \omega^{zy} + \frac{b_k}{\sqrt{N}} \sum_{z \notin C} \omega^{zy}$$

$$\begin{aligned}
&= \frac{1}{\sqrt{N}}(Ta_k + (N - T)b_k) \\
&= \frac{1}{\sqrt{N}} \left[\frac{T}{\sqrt{T}} \sin(2k + 1)\theta + \frac{N - T}{\sqrt{N - T}} \cos(2k + 1)\theta \right] \\
&= \sqrt{\frac{T}{N}} \sin(2k + 1)\theta + \sqrt{1 - \frac{T}{N}} \cos(2k + 1)\theta \\
&= \sin \theta \sin(2k + 1)\theta + \cos \theta \cos(2k + 1)\theta \\
&= \cos(2k\theta)
\end{aligned}$$

We have

$$\Pr(y = 0) = \cos^2(2k\theta)$$

Lemma 19.

$$\frac{4T}{N}(1 - \frac{T}{N}) = \sin^2 2\theta \geq \Pr(y = 0) = \cos^2 2k\theta \geq 0$$

Proof. Using $k = \lfloor \frac{\pi}{4\theta} \rfloor \implies \frac{\pi}{4\theta} - 1 \leq k \leq \frac{\pi}{4\theta} \implies \frac{\pi}{2} - 2\theta \leq 2k\theta \leq \frac{\pi}{2} \implies \sin(2\theta) = \cos(\frac{\pi}{2} - 2\theta) \geq \cos 2k\theta \geq \cos \frac{\pi}{2} = 0$ we have

$$\sin 2\theta = 2 \sin \theta \cos \theta = 2\sqrt{\frac{T}{N}}\sqrt{1 - \frac{T}{N}}$$

□

3.4.2 Amplified-QFT Analysis: $Py = 0 \bmod N, y \neq 0$

By making use of previous lemmas we have

$$\begin{aligned}
\text{Amp}(y) &= \frac{(a_k - b_k)}{\sqrt{N}} \left[\omega^{sy} \sum_{r=0}^{M-1} \omega^{rPy} + \sum_{z \in G} \omega^{zy} \right] + \frac{b_k}{\sqrt{N}} \sum_{z=0}^{N-1} \omega^{zy} \\
&= \frac{(a_k - b_k)}{\sqrt{N}} \left[\omega^{sy} \sum_{r=0}^{M-1} \omega^{rPy} + \sum_{z \in G} \omega^{zy} \right]
\end{aligned}$$

$$\begin{aligned}
&= \frac{(a_k - b_k)}{\sqrt{N}} \left[\omega^{sy} M + \sum_{z \in G} \omega^{zy} \right] \\
&= \frac{T(a_k - b_k)}{\sqrt{N}} \left[\frac{M}{T} \omega^{sy} + \frac{1}{T} \sum_{z \in G} \omega^{zy} \right] \\
&= \tan \theta \sin 2k\theta \left[\frac{M}{T} \omega^{sy} + \frac{1}{T} \sum_{z \in G} \omega^{zy} \right]
\end{aligned}$$

Therefore by the following lemma we have this result for the $\Pr(y)$:

$$\begin{aligned}
\Pr(y) &= \tan^2 \theta \sin^2 2k\theta \left| \frac{M}{T} \omega^{sy} + \frac{1}{T} \sum_{z \in G} \omega^{zy} \right|^2 \\
&\leq \tan^2 \theta \sin^2 2k\theta
\end{aligned}$$

Lemma 20. $\left| \frac{M}{T} \omega^{sy} + \frac{1}{T} \sum_{z \in G} \omega^{zy} \right|^2 \leq 1$

Proof.

$$\begin{aligned}
&\left| \frac{M}{T} \omega^{sy} + \frac{1}{T} \sum_{z \in G} \omega^{zy} \right|^2 \\
&\leq \left| \frac{M}{T} \omega^{sy} \right|^2 + \left| 2 \frac{M}{T} \omega^{sy} \frac{1}{T} \sum_{z \in G} \omega^{zy} \right| + \left| \frac{1}{T} \sum_{z \in G} \omega^{zy} \right|^2 \\
&\leq \frac{M^2}{T^2} + \frac{2ML}{T^2} + \frac{L^2}{T^2} \\
&= 1
\end{aligned}$$

□

3.4.3 Amplified-QFT Analysis: $Py \neq 0 \pmod{N}$

Making use of the previous lemmas we have

$$\text{Amp}(y) = \frac{(a_k - b_k)}{\sqrt{N}} \left[\omega^{sy} \sum_{r=0}^{M-1} \omega^{rPy} + \sum_{z \in G} \omega^{zy} \right] + \frac{b_k}{\sqrt{N}} \sum_{z=0}^{N-1} \omega^{zy}$$

$$\begin{aligned}
&= \frac{(a_k - b_k)}{\sqrt{N}} \left[\omega^{sy} \sum_{r=0}^{M-1} \omega^{rPy} + \sum_{z \in G} \omega^{zy} \right] \\
&= \frac{(a_k - b_k)}{\sqrt{N}} \left[\omega^{sy} \left[\frac{1 - \omega^{MPy}}{1 - \omega^{Py}} \right] + \sum_{z \in G} \omega^{zy} \right] \\
&= \frac{T(a_k - b_k)}{\sqrt{N}} \left[\frac{1}{T} \omega^{sy} \left[\frac{1 - \omega^{MPy}}{1 - \omega^{Py}} \right] + \frac{1}{T} \sum_{z \in G} \omega^{zy} \right] \\
&= \tan \theta \sin 2k\theta \left[\frac{1}{T} \omega^{sy} \left[\frac{1 - \omega^{MPy}}{1 - \omega^{Py}} \right] + \frac{1}{T} \sum_{z \in G} \omega^{zy} \right]
\end{aligned}$$

Therefore by the following lemma we have this result for the $\Pr(y)$:

$$\begin{aligned}
\Pr(y) &= \tan^2 \theta \sin^2 2k\theta \left| \frac{1}{T} \omega^{sy} \left[\frac{1 - \omega^{MPy}}{1 - \omega^{Py}} \right] + \frac{1}{T} \sum_{z \in G} \omega^{zy} \right|^2 \\
&\leq \tan^2 \theta \sin^2 2k\theta
\end{aligned}$$

Lemma 21. $\left| \frac{1}{T} \omega^{sy} \left[\frac{1 - \omega^{MPy}}{1 - \omega^{Py}} \right] + \frac{1}{T} \sum_{z \in G} \omega^{zy} \right|^2 \leq 1$

Proof.

$$\begin{aligned}
&\left| \frac{1}{T} \omega^{sy} \left[\frac{1 - \omega^{MPy}}{1 - \omega^{Py}} \right] + \frac{1}{T} \sum_{z \in G} \omega^{zy} \right|^2 \\
&\leq \left| \frac{1}{T} \omega^{sy} \left[\frac{1 - \omega^{MPy}}{1 - \omega^{Py}} \right] \right|^2 + 2 \left| \frac{1}{T} \omega^{sy} \left[\frac{1 - \omega^{MPy}}{1 - \omega^{Py}} \right] \right| \left| \frac{1}{T} \sum_{z \in G} \omega^{zy} \right| + \left| \frac{1}{T} \sum_{z \in G} \omega^{zy} \right|^2 \\
&\leq \frac{1}{T^2} \left| \frac{\sin(\pi MPy/N)}{\sin(\pi Py/N)} \right|^2 + \frac{2L}{T^2} \left| \frac{\sin(\pi MPy/N)}{\sin(\pi Py/N)} \right| + \frac{L^2}{T^2} \\
&\leq \frac{M^2}{T^2} + \frac{2LM}{T^2} + \frac{L^2}{T^2} \\
&= 1
\end{aligned}$$

□

We notice that if in addition $MPy = 0 \pmod N$ then

$$\begin{aligned}
\Pr(y) &= \tan^2 \theta \sin^2 2k\theta \left| \frac{1}{T} \sum_{z \in G} \omega^{zy} \right|^2 \\
&\leq \frac{L^2}{T^2} \tan^2 \theta \sin^2 2k\theta
\end{aligned}$$

3.4.4 Amplified-QFT Summary

The probability $\Pr(y)$ is given exactly by

$$\left\{ \begin{array}{l} \text{Case A: } \cos^2 2k\theta \\ \text{Case B: } \tan^2 \theta \sin^2 2k\theta \left| \frac{M}{T} \omega^{sy} + \frac{1}{T} \sum_{z \in G} \omega^{zy} \right|^2 \\ \text{Case C: } \tan^2 \theta \sin^2 2k\theta \left| \frac{1}{T} \omega^{sy} \left[\frac{1 - \omega^{MPy}}{1 - \omega^{Py}} \right] + \frac{1}{T} \sum_{z \in G} \omega^{zy} \right|^2 \\ \text{Case D: } \tan^2 \theta \sin^2 2k\theta \left| \frac{1}{T} \sum_{z \in G} \omega^{zy} \right|^2 \end{array} \right\}$$

3.5 Applying the QFT to the Oracle.

In this section we just apply the QFT to the binary Oracle h , which is 1 on C and 0 elsewhere.

We begin with the following state

$$|\xi\rangle = \frac{1}{\sqrt{N}} \sum_{z=0}^{N-1} |z\rangle \otimes \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle)$$

and apply the unitary transform for h , U_h , to this state which performs the following action:

$$U_h|z\rangle|c\rangle=|z\rangle|c\oplus h(z)\rangle$$

to get the state $|\psi\rangle$

$$\begin{aligned} |\psi\rangle &= U_h \frac{1}{\sqrt{N}} \sum_{z=0}^{N-1} |z\rangle \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle) \\ &= \frac{1}{\sqrt{N}} \left[(-1) \sum_{z \in C} |z\rangle + \sum_{z \notin C} |z\rangle \right] \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle) \\ &= \frac{1}{\sqrt{N}} \left[(-2) \sum_{z \in C} |z\rangle + \sum_{z=0}^{N-1} |z\rangle \right] \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle) \\ &= \frac{1}{\sqrt{N}} \left[(-2) \sum_{z \in A} |z\rangle - 2 \sum_{z \in G} |z\rangle + \sum_{z=0}^{N-1} |z\rangle \right] \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle) \end{aligned}$$

Next we apply the QFT to try to find the period P , dropping $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$.

The QFT applies the following action:

$$|z\rangle \rightarrow \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} \omega^{zy} |y\rangle$$

to get

$$\begin{aligned} |\phi\rangle &= \sum_{y=0}^{N-1} \left[\frac{-2}{N} \sum_{z \in C} \omega^{zy} + \frac{1}{N} \sum_{z=0}^{N-1} \omega^{zy} \right] |y\rangle \\ &= \sum_{y=0}^{N-1} \left[\frac{-2}{N} \sum_{z \in A} \omega^{zy} - \frac{2}{N} \sum_{z \in G} \omega^{zy} + \frac{1}{N} \sum_{z=0}^{N-1} \omega^{zy} \right] |y\rangle \\ &= \sum_{y=0}^{N-1} \left[\frac{-2}{N} \omega^{sy} \sum_{r=0}^{M-1} \omega^{rPy} - \frac{2}{N} \sum_{z \in G} \omega^{zy} + \frac{1}{N} \sum_{z=0}^{N-1} \omega^{zy} \right] |y\rangle \end{aligned}$$

3.5.1 QFT Analysis: $y = 0$

We have

$$\begin{aligned}
Amp(y) &= \frac{(-2)}{N} \sum_{z \in C} \omega^{zy} + \frac{1}{N} \sum_{z=0}^{N-1} \omega^{zy} \\
&= \frac{-2T}{N} + \frac{N}{N} \\
&= 1 - \frac{2T}{N}
\end{aligned}$$

Therefore, in the QFT case, we have $\Pr(y = 0)$ is very close to 1 and is given by

$$\Pr(y = 0) = \left(1 - \frac{2T}{N}\right)^2$$

whereas in the Amplified-QFT case we have $\Pr(y = 0)$ is given by

$$\Pr(y = 0) = \cos^2 2k\theta$$

3.5.2 QFT Analysis: $Py = 0 \bmod N, y \neq 0$

Using previous lemmas we have

$$\begin{aligned}
Amp(y) &= \frac{-2}{N} \omega^{sy} \sum_{r=0}^{M-1} \omega^{rPy} - \frac{2}{N} \sum_{z \in G} \omega^{zy} + \frac{1}{N} \sum_{z=0}^{N-1} \omega^{zy} \\
&= \frac{-2}{N} \omega^{sy} \sum_{r=0}^{M-1} \omega^{rPy} - \frac{2}{N} \sum_{z \in G} \omega^{zy} \\
&= \frac{-2}{N} \left[\omega^{sy} M + \sum_{z \in G} \omega^{zy} \right]
\end{aligned}$$

Therefore in the QFT case we have $\Pr(y)$ is given by

$$\Pr(y) = \frac{4}{N^2} \left| \omega^{sy} M + \sum_{z \in G} \omega^{zy} \right|^2$$

$$\leq \frac{4T^2}{N^2}$$

whereas in the Amplified-QFT case we have $\Pr(y)$ is given by

$$\Pr(y) = \tan^2 \theta \sin^2 2k\theta \left| \frac{M}{T} \omega^{sy} + \frac{1}{T} \sum_{z \in G} \omega^{zy} \right|^2$$

We can determine how the increase in amplitude varies with the number of iterations k of the Grover step in the Amplified-QFT by examining the ratio of the amplitudes of the Amplified-QFT case and QFT case. This ratio is given exactly by

$$\begin{aligned} \text{AmpRatio}(y) &= \frac{\tan \theta \sin 2k\theta \left[\frac{M}{T} \omega^{sy} + \frac{1}{T} \sum_{z \in G} \omega^{zy} \right]}{\frac{-2}{N} [\omega^{sy} M + \sum_{z \in G} \omega^{zy}]} \\ &= \frac{N}{-2T} \tan \theta \sin 2k\theta \end{aligned}$$

We also have the following inequality for the $\Pr \text{Ratio}(y)$, the increase in the probability due to amplification:

$$\begin{aligned} \frac{N}{4T} \left(\frac{N}{N-T} \right) &\geq \Pr \text{Ratio}(y) \geq \frac{N}{4T} \left(\frac{N}{N-T} \right) \left(1 - \frac{2T}{N} \right)^2 \\ &\implies \Pr \text{Ratio}(y) \approx \frac{N}{4T} \end{aligned}$$

3.5.3 QFT Analysis: $Py \neq 0 \bmod N$

We have

$$\begin{aligned} \text{Amp}(y) &= \frac{-2}{N} \omega^{sy} \sum_{r=0}^{M-1} \omega^{rPy} - \frac{2}{N} \sum_{z \in G} \omega^{zy} + \frac{1}{N} \sum_{z=0}^{N-1} \omega^{zy} \\ &= \frac{-2}{N} \omega^{sy} \sum_{r=0}^{M-1} \omega^{rPy} - \frac{2}{N} \sum_{z \in G} \omega^{zy} \\ &= \frac{-2}{N} \omega^{sy} \left[\frac{1 - \omega^{MPy}}{1 - \omega^{Py}} \right] - \frac{2}{N} \sum_{z \in G} \omega^{zy} \end{aligned}$$

In the QFT case, we have $\Pr(y)$ is given by

$$\begin{aligned}
\Pr(y) &= \frac{4}{N^2} \left| w^{sy} \left[\frac{1 - \omega^{MPy}}{1 - \omega^{Py}} \right] + \sum_{z \in G} \omega^{zy} \right|^2 \\
&\leq \frac{4}{N^2} \left| w^{sy} \left| \frac{\sin(\pi MPy/N)}{\sin(\pi Py/N)} \right| + \sum_{z \in G} \omega^{zy} \right|^2 \\
&\leq \frac{4}{N^2} [M + L]^2 \\
&\leq \frac{4T^2}{N^2}
\end{aligned}$$

whereas in the Amplified-QFT case we have $\Pr(y)$ is given by

$$\Pr(y) = \tan^2 \theta \sin^2 2k\theta \left| \frac{1}{T} w^{sy} \left[\frac{1 - \omega^{MPy}}{1 - \omega^{Py}} \right] + \frac{1}{T} \sum_{z \in G} \omega^{zy} \right|^2$$

The ratio of the amplitudes of the Amplified-QFT case and QFT case is given exactly by

$$\begin{aligned}
\text{AmpRatio}(y) &= \frac{\tan \theta \sin 2k\theta \left[\frac{1}{T} w^{sy} \left[\frac{1 - \omega^{MPy}}{1 - \omega^{Py}} \right] + \frac{1}{T} \sum_{z \in G} \omega^{zy} \right]}{\frac{-2}{N} w^{sy} \left[\frac{1 - \omega^{MPy}}{1 - \omega^{Py}} \right] - \frac{2}{N} \sum_{z \in G} \omega^{zy}} \\
&= \frac{N}{-2T} \tan \theta \sin 2k\theta
\end{aligned}$$

We note that this ratio is the same as in that given in the previous section and is independent of y . The variables in this ratio do not depend in anyway on the QFT. We also have the following inequality for the $\Pr \text{Ratio}(y)$, the increase in the probability due to amplification:

$$\begin{aligned}
\frac{N}{4T} \left(\frac{N}{N-T} \right) &\geq \Pr \text{Ratio}(y) \geq \frac{N}{4T} \left(\frac{N}{N-T} \right) \left(1 - \frac{2T}{N} \right)^2 \\
&\implies \Pr \text{Ratio}(y) \approx \frac{N}{4T}
\end{aligned}$$

We notice that if in addition $MPy = 0 \bmod N$ then

$$\begin{aligned}\Pr(y) &= \frac{4}{N^2} \left| \sum_{z \in G} \omega^{zy} \right|^2 \\ &\leq \frac{4L^2}{N^2}\end{aligned}$$

3.5.4 QFT Summary

The probability $\Pr(y)$ is given exactly by

$$\left\{ \begin{array}{l} \text{Case A: } \left(1 - \frac{2T}{N}\right)^2 \\ \\ \text{Case B: } \frac{4}{N^2} \left| \omega^{sy} M + \sum_{z \in G} \omega^{zy} \right|^2 \\ \\ \text{Case C: } \frac{4}{N^2} \left| w^{sy} \left[\frac{1 - \omega^{MPy}}{1 - \omega^{Py}} \right] + \sum_{z \in G} \omega^{zy} \right|^2 \\ \\ \text{Case D: } \frac{4}{N^2} \left| \sum_{z \in G} \omega^{zy} \right|^2 \end{array} \right\}$$

3.6 Applying the QHS to the Oracle

In this section we provide the calculations for the probabilities of success for the QHS algorithm. The QHS algorithm is a two register algorithm as follows (see ref[13] for details). We begin with $|0\rangle > |0\rangle$ where the first register is n qubits and the second register is 1 qubit and apply the Hadamard transform to the first register to get a uniform superposition state, followed by the unitary transformation for the

Oracle h to get:

$$|\psi\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle |h(x)\rangle$$

Next we apply the QFT to the first register to get

$$\begin{aligned} |\psi\rangle &= \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} \omega^{xy} |y\rangle |h(x)\rangle \\ &= \sum_{y=0}^{N-1} \frac{1}{N} \sum_{x=0}^{N-1} \omega^{xy} |y\rangle |h(x)\rangle \\ &= \sum_{y=0}^{N-1} \frac{1}{N} |y\rangle \sum_{x=0}^{N-1} \omega^{xy} |h(x)\rangle \\ &= \sum_{y=0}^{N-1} \frac{||\Gamma(y)\rangle||}{N} |y\rangle \frac{|\Gamma(y)\rangle}{||\Gamma(y)\rangle||} \end{aligned}$$

where

$$\begin{aligned} |\Gamma(y)\rangle &= \sum_{x=0}^{N-1} \omega^{xy} |h(x)\rangle \\ &= \sum_{x \in C} \omega^{xy} |1\rangle + \sum_{x \notin C} \omega^{xy} |0\rangle \end{aligned}$$

and where

$$||\Gamma(y)\rangle||^2 = \left| \sum_{x \in C} \omega^{xy} \right|^2 + \left| \sum_{x \notin C} \omega^{xy} \right|^2$$

Next we make a measurement to get y and find that the probability of this measurement is

$$\begin{aligned} \Pr(y) &= \frac{||\Gamma(y)\rangle||^2}{N^2} \\ &= \frac{1}{N^2} \left| \sum_{x \in C} \omega^{xy} \right|^2 + \frac{1}{N^2} \left| \sum_{x \notin C} \omega^{xy} \right|^2 \end{aligned}$$

The state that we end up in is of the form

$$|\phi\rangle = |y\rangle \frac{|\Gamma(y)\rangle}{\| |\Gamma(y)\rangle \|}$$

So now we are interested in the probability of measuring y in the usual cases in order to recover the period P .

3.6.1 QHS Analysis: $y = 0$

We have

$$\begin{aligned} \Pr(y) &= \frac{1}{N^2} \left| \sum_{x \in C} \omega^{xy} \right|^2 + \frac{1}{N^2} \left| \sum_{x \notin C} \omega^{xy} \right|^2 \\ &= \frac{T^2}{N^2} + \frac{(N-T)^2}{N^2} = \frac{T^2 + N^2 - 2NT + T^2}{N^2} \\ &= 1 - \frac{2T(N-T)}{N^2} \end{aligned}$$

whereas in the Amplified-QFT case we have $\Pr(y = 0)$ is given by

$$\Pr(y = 0) = \cos^2 2k\theta$$

3.6.2 QHS Analysis: $Py = 0 \pmod N, y \neq 0$

We have

$$\begin{aligned} \Pr(y) &= \frac{1}{N^2} \left| \sum_{x \in C} \omega^{xy} \right|^2 + \frac{1}{N^2} \left| \sum_{x \notin C} \omega^{xy} \right|^2 \\ &= \frac{1}{N^2} \left| \omega^{sy} \sum_{r=0}^{M-1} \omega^{rPy} + \sum_{x \in G} \omega^{xy} \right|^2 + \frac{1}{N^2} \left| \sum_{x \notin C} \omega^{xy} \right|^2 \\ &= \frac{1}{N^2} \left| \omega^{sy} M + \sum_{x \in G} \omega^{xy} \right|^2 + \frac{1}{N^2} \left| -\omega^{sy} M - \sum_{x \in G} \omega^{xy} + \frac{1}{N} \sum_{x=0}^{N-1} \omega^{xy} \right|^2 \end{aligned}$$

$$\begin{aligned}
&= \frac{2}{N^2} \left| \omega^{sy} M + \sum_{x \in G} \omega^{xy} \right|^2 \\
&\leq \frac{2T^2}{N^2}
\end{aligned}$$

In the Amplified-QFT case we have $\Pr(y)$ is given by

$$\Pr(y) = \tan^2 \theta \sin^2 2k\theta \left| \frac{M}{T} \omega^{sy} + \frac{1}{T} \sum_{z \in G} \omega^{zy} \right|^2$$

By comparing the results of the QHS and the Amplified-QFT algorithms we have the following inequality for the $\Pr Ratio(y) = \Pr(y)_{\text{Amplified-QFT}} / \Pr(y)_{\text{QHS}}$, the increase in the probability due to amplification

$$\begin{aligned}
\Pr Ratio(y) &= \frac{\tan^2 \theta \sin^2 2k\theta \left| \frac{M}{T} \omega^{sy} + \frac{1}{T} \sum_{z \in G} \omega^{zy} \right|^2}{\frac{2}{N^2} \left| \omega^{sy} M + \sum_{x \in G} \omega^{xy} \right|^2} \\
&= \frac{N^2}{2T^2} \tan^2 \theta \sin^2 2k\theta
\end{aligned}$$

which gives

$$\begin{aligned}
\frac{N}{2T} \left(\frac{N}{N-T} \right) &\geq \Pr Ratio(y) \geq \frac{N}{2T} \left(\frac{N}{N-T} \right) \left(1 - \frac{2T}{N} \right)^2 \\
&\implies \Pr Ratio(y) \approx \frac{N}{2T}
\end{aligned}$$

3.6.3 QHS Analysis: $Py \neq 0 \pmod N$

We have

$$\Pr(y) = \frac{1}{N^2} \left| \omega^{sy} M + \sum_{x \in G} \omega^{xy} \right|^2 + \frac{1}{N^2} \left| -\omega^{sy} M - \sum_{x \in G} \omega^{xy} + \frac{1}{N} \sum_{x=0}^{N-1} \omega^{xy} \right|^2$$

$$\begin{aligned}
&= \frac{2}{N^2} \left| \omega^{sy} \sum_{r=0}^{M-1} \omega^{rPy} + \sum_{x \in G} \omega^{xy} \right|^2 \\
&= \frac{2}{N^2} \left| \omega^{sy} \left[\frac{1 - \omega^{MPy}}{1 - \omega^{Py}} \right] + \sum_{x \in G} \omega^{xy} \right|^2 \\
&\leq \frac{2}{N^2} \left| \omega^{sy} \left| \frac{\sin(\pi MPy/N)}{\sin(\pi Py/N)} \right| + \sum_{x \in G} \omega^{xy} \right|^2 \\
&\leq \frac{2}{N^2} [M + L]^2 \\
&\leq \frac{2T^2}{N^2}
\end{aligned}$$

In the Amplified-QFT case we have $\Pr(y)$ is given by

$$\Pr(y) = \tan^2 \theta \sin^2 2k\theta \left| \frac{1}{T} \omega^{sy} \left[\frac{1 - \omega^{MPy}}{1 - \omega^{Py}} \right] + \frac{1}{T} \sum_{z \in G} \omega^{zy} \right|^2$$

By comparing the results of the QHS and the Amplified-QFT algorithms we have the following inequality for the $\Pr Ratio(y) = \Pr(y)_{Amplified-QFT} / \Pr(y)_{QHS}$, the increase in the probability due to amplification

$$\begin{aligned}
\Pr Ratio(y) &= \frac{\tan^2 \theta \sin^2 2k\theta \left| \frac{1}{T} \omega^{sy} \left[\frac{1 - \omega^{MPy}}{1 - \omega^{Py}} \right] + \frac{1}{T} \sum_{z \in G} \omega^{zy} \right|^2}{\frac{2}{N^2} \left| \omega^{sy} \left[\frac{1 - \omega^{MPy}}{1 - \omega^{Py}} \right] + \sum_{x \in G} \omega^{xy} \right|^2} \\
&= \frac{N^2}{2T^2} \tan^2 \theta \sin^2 2k\theta
\end{aligned}$$

which gives

$$\begin{aligned}
\frac{N}{2T} \left(\frac{N}{N-T} \right) &\geq \Pr Ratio(y) \geq \frac{N}{2T} \left(\frac{N}{N-T} \right) \left(1 - \frac{2T}{N} \right)^2 \\
&\implies \Pr Ratio(y) \approx \frac{N}{2T}
\end{aligned}$$

We notice that if in addition $MPy = 0 \bmod N$ then

$$\begin{aligned}\Pr(y) &= \frac{2}{N^2} \left| \sum_{z \in G} \omega^{zy} \right|^2 \\ &\leq \frac{2L^2}{N^2}\end{aligned}$$

3.6.4 QHS Summary

The $\Pr(y)$ in the QHS case is:

$$\left\{ \begin{array}{l} \text{Case A: } 1 - \frac{2T(N-T)}{N^2} \\ \text{Case B: } \frac{2}{N^2} \left| \omega^{sy} M + \sum_{z \in G} \omega^{zy} \right|^2 \\ \text{Case C: } \frac{2}{N^2} \left| w^{sy} \left[\frac{1 - \omega^{MPy}}{1 - \omega^{Py}} \right] + \sum_{z \in G} \omega^{zy} \right|^2 \\ \text{Case D: } \frac{2}{N^2} \left| \sum_{z \in G} \omega^{zy} \right|^2 \end{array} \right\}$$

Chapter 4: An Uncertainty Principle for the Amplified-QFT

In this chapter we show there is an uncertainty principle for the Amplified-QFT algorithm. This result provides a relationship between the support of the state vector after Grover's algorithm has been run and the support of the state vector after the QFT has been run. This result uses the results of Donoho and Stark found in ref[15], ref[16] and ref[17]. First we state and prove the Donoho and Stark lemma 1 from their paper which we will use to good effect for the Amplified-QFT case.

Lemma 22. *If $\{x_j\}$ $j = 0, 1, \dots, N - 1$ has T nonzero elements, then $\{y_k\}$ $k = 0, 1, \dots, N - 1$ cannot have T consecutive zeros, where $\{y_k\}$ is the discrete Fourier transform of $\{x_j\}$.*

Proof. Define

$$y_k = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} x_j w^{jk}$$

where $w = \exp(-2\pi i/N)$. Suppose there are T consecutive positions $\{y_{t+r}\}$ $r = 0, 1, \dots, T - 1$ which are all zero. Then we have a system of T equations each of which are zero as follows:

$$y_{t+r} = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} x_j w^{j(t+r)} = 0, r = 0, \dots, T - 1$$

However there are only T values of x_j which are nonzero. Let us call these positions

$S = \{s_j\} \ j = 0, 1, \dots, T-1$. Then we can rewrite our system of equations as follows:

$$y_{t+r} = \frac{1}{\sqrt{N}} \sum_{j=0}^{T-1} x_{s_j} w^{s_j(t+r)} = 0$$

Then we have a system of T equations in T unknowns equal to zero.

$$Zx = 0$$

However the vector x contains elements x_{s_j} which are all nonzero. Therefore the matrix Z must be singular. However we will show that Z is non-singular, thereby showing that we cannot have such a system of equations and cannot have T consecutive $y_k = 0$. Let us take a closer look at Z .

$$Z = \begin{bmatrix} w^{s_0 t} & w^{s_1 t} & \dots & w^{s_{T-1} t} \\ w^{s_0(t+1)} & w^{s_1(t+1)} & \dots & w^{s_{T-1}(t+1)} \\ \dots & \dots & \dots & \dots \\ w^{s_0(t+T-1)} & w^{s_1(t+T-1)} & \dots & w^{s_{T-1}(t+T-1)} \end{bmatrix}$$

We can consider an equivalent set of equations

$$ZPP^{-1}x = 0$$

where $P^{-1}x$ has all nonzero elements

$$P = \begin{bmatrix} w^{-s_0 t} & 0 & \dots & 0 \\ 0 & w^{-s_1 t} & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & w^{-s_{T-1} t} \end{bmatrix}$$

where ZP is given by

$$Z' = \begin{bmatrix} 1 & 1 & \dots & 1 \\ w^{s_0} & w^{s_1} & \dots & w^{s_{T-1}} \\ \dots & \dots & \dots & \dots \\ w^{s_0(T-1)} & w^{s_1(T-1)} & \dots & w^{s_{T-1}(T-1)} \end{bmatrix}$$

which can be rewritten as a Vandermonde matrix

$$V = \begin{bmatrix} 1 & 1 & \dots & 1 \\ \alpha_0 & \alpha_1 & \dots & \alpha_{T-1} \\ \dots & \dots & \dots & \dots \\ \alpha_0^{T-1} & \alpha_1^{T-1} & \dots & \alpha_{T-1}^{T-1} \end{bmatrix}$$

which is known to be nonsingular. □

Note that in the proof we can consider the positions to be taken mod N so that the $\{x_j\}$ and $\{y_k\}$ can be viewed as being on a circle. This takes into account that we cannot have T consecutive zeros wrapping around the endpoints.

If we cannot have T consecutive zeros in $\{y_k\}$ then the number of nonzero elements in $\{y_k\}$ must be at least N/T . For example, we could have $T - 1$ zeros followed by a single nonzero element in every T long block of $\{y_k\}$. Since there are N/T such blocks we have the following result:

Theorem 23. (*Donoho and Stark*) *Let $\{x_j\}$ $j = 0, 1, \dots, N - 1$ have N_x nonzero elements. Let $\{y_k\}$ $k = 0, 1, \dots, N - 1$ be the Fourier transform of $\{x_j\}$ with N_y nonzero elements. Then*

$$N_x N_y \geq N$$

Next we apply this to the quantum case. Consider the following state where $\{p_x\}$ is a probability distribution

$$|\psi_x\rangle = \sum_{x=0}^{N-1} \sqrt{p_x} |x\rangle$$

and apply the QFT which maps

$$|x\rangle \rightarrow \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} w^{xy} |y\rangle$$

to get the state

$$|\psi_y\rangle = \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} \sum_{x=0}^{N-1} \sqrt{p_x} w^{xy} |y\rangle$$

Suppose we have T of the $\sqrt{p_x}$ amplitudes of $|\psi_x\rangle$ nonzero at positions s_j , $j = 0, 1, \dots, T-1$ and suppose we have T consecutive amplitudes of $|\psi_y\rangle$ equal to zero, we have a system of T equations as in the lemma

$$y_{t+r} = \frac{1}{\sqrt{N}} \sum_{j=0}^{T-1} \sqrt{p_{s_j}} w^{s_j(t+r)} = 0, r = 0, 1, \dots, T-1$$

We see we can apply the lemma so that there are not T consecutive amplitudes of $|y\rangle$ in the state $|\psi_y\rangle$ that are all zero. Therefore if N_x is the number of nonzero amplitudes of $|\psi_x\rangle$ and N_y is the number of nonzero amplitudes of $|\psi_y\rangle$ then we have

$$N_x N_y \geq N$$

Next we apply this result to the Amplified-QFT algorithm. We recall that we have a set of labels $L = \{0, 1, \dots, N-1\}$ and an oracle $f : L \rightarrow \{0, 1\}$ which is

1 on a periodic subset of labels A of size M and 0 elsewhere. We apply Grover's algorithm without measurement to arrive at the following state (See Chapter 2)

where $k = \left\lfloor \frac{\pi}{4 \sin^{-1}(\sqrt{M/N})} \right\rfloor$ is the number of steps of the Grover iteration:

$$|\psi_x\rangle = a_k \sum_{x \in A} |x\rangle + b_k \sum_{x \notin A} |x\rangle$$

where

$$a_k = \frac{1}{\sqrt{M}} \sin(2k+1)\theta, b_k = \frac{1}{\sqrt{N-M}} \cos(2k+1)\theta$$

are the appropriate amplitudes of the states and where

$$\sin \theta = \sqrt{M/N}, \cos \theta = \sqrt{1 - M/N}$$

We note that the number of non-zero amplitudes is N because Grover's algorithm puts nearly all of the probability on the set A but leaves some residual probability on \bar{A} . In fact

$$p(A) \geq 1 - \frac{M}{N} \text{ and } p(\bar{A}) \leq \frac{M}{N}$$

However we can still produce an uncertainty relation. Next we apply the QFT to $|\psi_x\rangle$ to obtain the state $|\psi_y\rangle$

$$\begin{aligned} |\psi_y\rangle &= \sum_{y=0}^{N-1} \left[\frac{a_k}{\sqrt{N}} \sum_{x \in A} \omega^{xy} + \frac{b_k}{\sqrt{N}} \sum_{x \notin A} \omega^{xy} \right] |y\rangle \\ &= \sum_{y=0}^{N-1} \left[\frac{a_k - b_k}{\sqrt{N}} \sum_{x \in A} \omega^{xy} + \frac{b_k}{\sqrt{N}} \sum_{x=0}^{N-1} \omega^{xy} \right] |y\rangle \end{aligned}$$

Now, for $y \neq 0$ we have

$$\sum_{x=0}^{N-1} \omega^{xy} = 0$$

and the amplitude for $y \neq 0$ is given by an M term sum

$$\frac{a_k - b_k}{\sqrt{N}} \sum_{x \in A} \omega^{xy}$$

where $a_k - b_k \neq 0$.

Consider the following system of M equations

$$y_{t+r} = \frac{1}{\sqrt{N}} \sum_{j=0}^{M-1} \sqrt{p_{x_j}} w^{x_j(t+r)} = 0, r = 0, 1, \dots, M-1$$

where $A = \{x_0, x_1, \dots, x_{M-1}\}$ and $\sqrt{p_{x_j}} = a_k - b_k$.

We see we can apply the lemma so that there are not M consecutive amplitudes of $|y\rangle$ in the state $|\psi_y\rangle$ that are all zero. Therefore the number of nonzero amplitudes of $|\psi_y\rangle$ must be at least N/M . Therefore if $|A| = M$ and N_y is the number of nonzero amplitudes of $|\psi_y\rangle$ then we have

$$MN_y \geq N$$

where M is the number of the largest nonzero amplitudes of $|\psi_x\rangle$. If Grover's algorithm worked perfectly M would be exactly the number of nonzero amplitudes of $|\psi_x\rangle$. However since it works imperfectly, M is the number of elements whose probabilities are $> 1/N$

Chapter 5: The Amplified-Haar Wavelet Transform

5.1 Introduction

In the Deutsch-Jozsa problem we are given a function which is either constant (all zeros or all ones) or balanced (is zeros half the time and ones half the time). This problem is easily solved using the Hadamard transform followed by a measurement. In this chapter we generalize this problem to consider the Local Constant or Balanced Signal Decision Problem and we generalize the idea of the amplified quantum Fourier transform in ref[14] to consider another amplified quantum transform - the amplified 1-d Haar wavelet transform (ref 44).

Let $L = \{0, 1, \dots, N - 1\}$ be a set of $N = 2^n$ labels and let $2M \ll N$. Let

$$A = \bigcup_{i \in E} A_i$$

be a subset of L of size $2M$, where E is any set of M even labels from L , and

$A_i = \{i, i + 1\}, i \in E$ are sets of consecutive labels and $A_i \cap A_j = \emptyset$. Let

$$f : L \rightarrow \{0, 1\}$$

be an oracle which is 1 on A and 0 elsewhere. Let

$$S : L \rightarrow \{0, 1\}$$

be a signal. We wish to solve the following problem:

the **Local Constant or Balanced Signal Decision Problem**. *We wish to determine which of the following two possibilities are the case:*

a) *On each A_i we can have $S(i) = 0$ and $S(i + 1) = 1$ or $S(i) = 1$ and $S(i + 1) = 0$ - this corresponds to the signal S being balanced on each A_i*

or

b) *On each A_i , $S(i) = 0$ and $S(i + 1) = 0$ or $S(i) = 1$ and $S(i + 1) = 1$ - this corresponds to the signal S being constant on each A_i .*

The value of the signal S on $L \setminus A$ can be any value in $\{0, 1\}$.

To solve the Local Constant or Balanced Signal Decision Problem, we first run Grover's algorithm to amplify the amplitudes on the set A by using the Oracle f . We then put the signal S into the amplitudes as $+/-1$ values and then run the Haar Wavelet Transform on the resulting state. In the case a) above, we will find that most of the probability lies in the following interval of labels $[N/2, N - 1]$. In case b) above, we will find that most of the probability lies in the following interval $[0, N/2 - 1]$. Therefore if we make a measurement with respect to the standard basis we can verify which interval the measurement lies and discover whether a) is the case or b) is the case. This algorithm works because of the special construction of the Haar matrix, which computes sums and differences between successive values on the even cut and puts the result in the upper half interval.

The Haar wavelet transform W of dimension 2^n by 2^n has the following form:

$W = W_n W_{n-1} \dots W_1$ where each W_k is defined as

$$W_k = \begin{bmatrix} H_k & 0 \\ 0 & I_k \end{bmatrix}$$
 where H_k is of dimension 2^{n-k+1} by 2^{n-k+1} and I_k is the identity matrix of dimension $2^n - 2^{n-k+1}$ by $2^n - 2^{n-k+1}$ and O is the all zero matrix of the appropriate dimension,

where

$$H_k = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 & 0 & 0 & \dots & 0 \\ 0 & 0 & 1 & 1 & \dots & \dots \\ \vdots & \vdots & \vdots & \vdots & \vdots & 0 & 0 \\ 0 & 0 & \dots & 0 & 1 & 1 \\ 1 & -1 & 0 & 0 & \dots & 0 \\ 0 & 0 & 1 & -1 & \dots & \dots \\ \vdots & \vdots & \vdots & \vdots & \vdots & 0 & 0 \\ 0 & 0 & \dots & 0 & 1 & -1 \end{bmatrix}$$

For example, consider W of dimension 2^2 by 2^2 then we have

$$W = \begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 & 0 \\ \frac{1}{\sqrt{2}} & \frac{-1}{\sqrt{2}} & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & -1 \end{bmatrix}$$

Consider the example of Wx where $x = \frac{1}{2}[1, 1, 1, 1]^T$

We have

$$Wx = \begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 & 0 \\ \frac{1}{\sqrt{2}} & \frac{-1}{\sqrt{2}} & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & -1 \end{bmatrix} \frac{1}{2} \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \end{bmatrix}$$

$$= \frac{1}{2\sqrt{2}} \begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 & 0 \\ \frac{1}{\sqrt{2}} & \frac{-1}{\sqrt{2}} & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 2 \\ 2 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}$$

where the result is in the upper half as expected.

Next consider the example of Wx where $x = \frac{1}{2}[1, -1, 1, -1]^T$

We have

$$Wx = \begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 & 0 \\ \frac{1}{\sqrt{2}} & \frac{-1}{\sqrt{2}} & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & -1 \end{bmatrix} \frac{1}{2} \begin{bmatrix} 1 \\ -1 \\ 1 \\ -1 \end{bmatrix}$$

$$= \frac{1}{2\sqrt{2}} \begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 & 0 \\ \frac{1}{\sqrt{2}} & \frac{-1}{\sqrt{2}} & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 0 \\ 0 \\ 2 \\ 2 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 0 \\ 0 \\ 1 \\ 1 \end{bmatrix}$$

where the results are in the lower half as expected.

5.2 The Local Constant or Balanced Signal Decision Problem-Analysis

The Amplified-Haar algorithm which solves the Local Constant or Balanced Signal Decision Problem is defined by the following four step procedure.

Step 1: Apply all of Grover's algorithm in its entirety except for the last measurement step to the starting state $|0\rangle$. The resulting state is given by $|\psi_k\rangle$

where $k = \left\lfloor \frac{\pi}{4 \sin^{-1}(\sqrt{2M/N})} \right\rfloor$:

$$|\psi_k\rangle = a_k \sum_{z \in A} |z\rangle + b_k \sum_{z \notin A} |z\rangle$$

where

$$a_k = \frac{1}{\sqrt{2M}} \sin(2k+1)\theta, b_k = \frac{1}{\sqrt{N-2M}} \cos(2k+1)\theta$$

are the appropriate amplitudes of the states and where

$$\sin \theta = \sqrt{2M/N}, \cos \theta = \sqrt{1 - 2M/N}$$

Step 2: We apply the signal S to an auxiliary qubit $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ added onto $|\psi_k\rangle$ to put the signal into the amplitudes of the state $|\psi_k\rangle$ to get the state $|\lambda_k\rangle$ where

$$|\lambda_k\rangle = a_k \sum_{z \in A} (-1)^{S(z)} |z\rangle + b_k \sum_{z \notin A} (-1)^{S(z)} |z\rangle$$

Step 3: We apply the Haar wavelet transform W to the resulting state $|\lambda_k\rangle$.

Step 4: We make a measurement z and note which range the measured value is in to determine the solution of the problem. If z is in $[0, N/2 - 1]$ then the signal was constant on each A_i otherwise the signal was balanced on each A_i .

Now we have,

$$\begin{aligned} k = \left\lfloor \frac{\pi}{4\theta} \right\rfloor &\implies \frac{\pi}{4\theta} - 1 \leq k \leq \frac{\pi}{4\theta} \implies \frac{\pi}{2} - \theta \leq (2k+1)\theta \leq \frac{\pi}{2} + \theta \\ &\implies \sin \theta = \cos(\frac{\pi}{2} - \theta) \geq \cos(2k+1)\theta \geq \cos(\frac{\pi}{2} + \theta) = -\sin \theta \end{aligned}$$

Notice that the total probability of the $N - 2M$ labels that are not in A is

$$\begin{aligned}
(N - 2M) \left(\frac{1}{\sqrt{N - 2M}} \cos(2k + 1)\theta \right)^2 &= \cos^2(2k + 1)\theta \\
\implies \cos^2(2k + 1)\theta &\leq \sin^2 \theta = \sin^2(\sin^{-1}(\sqrt{\frac{2M}{N}})) \\
\implies \cos^2(2k + 1)\theta &\leq \frac{2M}{N}
\end{aligned}$$

whereas the total probability of the $2M$ labels in A is

$$\begin{aligned}
2M \left(\frac{1}{\sqrt{2M}} \sin(2k + 1)\theta \right)^2 &= \sin^2(2k + 1)\theta = 1 - \cos^2(2k + 1)\theta \\
\implies \sin^2(2k + 1)\theta &\geq 1 - \frac{2M}{N}
\end{aligned}$$

We notice that in Step 3, after we have applied the first orthogonal transform W_1 of W we have essentially solved our problem. If the signal is constant on A then the total probability of the labels in $[0, N/2 - 1]$ is at least $\frac{1}{2}M(a_k + a_k)^2 = 2M(\frac{1}{\sqrt{2M}} \sin(2k + 1)\theta)^2 = \sin^2(2k + 1)\theta \geq 1 - \frac{2M}{N}$. So we have moved most of the probability of the set A to the lower half range of labels. Similarly if the signal is balanced on A then this probability would be moved to the upper half range of labels $[N/2, N - 1]$. The successive remaining orthogonal transforms $W_n \dots W_2$ do not move the probabilities outside of these ranges. So we see we need only apply W_1 to solve this problem and make a measurement. The work factor of this algorithm is dominated by the Grover step and which is $O(\sqrt{\frac{N}{2M}})$.

A classical solution to this problem would be to randomly choose labels x in the range $[0, N - 1]$ and to verify that $f(x) = 1$. If x is even then we check the values of $s(x)$ and $s(x + 1)$ to see what kind of signal we have. If x is odd, we check $s(x)$ and $s(x - 1)$. This procedure has workfactor $O(N/2M)$ showing that the

amplified-Haar wavelet transform is quadratically faster.

In order to consider a quantum algorithm that would solve the Local Constant or Balanced Signal Problem without using amplification, we need to consider the values of the signal on the set $L \setminus A$. We can consider the following problem where we want to find out which situation is the case:

a) The set A is constant and the set $L \setminus A$ is balanced

or

b) The set A is balanced and the set $L \setminus A$ is constant.

Suppose we perform the Haar transform on the signal S corresponding to these situations and make a measurement. Regardless of which case we are in, if the measured value is in the interval $[0, N/2 - 1]$ we have measured a value due to the probability of the constant part of the signal, whereas if we measure a value in the range $[N/2, N - 1]$ we have measured a value due to the probability of the balanced part of the signal. We are performing sampling of a probability distribution and we need to determine which case we are in. If we repeat this process we can estimate the means of the Binomial probability distributions we are sampling from.

What are the means and variances of the Binomial distributions we are sampling from?

Letting p be probability of the constant signal and q be the probability of the balanced signal we have:

case a) $p_a = M/N$ and $q_a = 1 - M/N$ with variance $\sigma^2 = Np_aq_a = M(1 - M/N)$

and in

case b) $p_b = 1 - M/N$ and $q_b = M/N$ with variance $\sigma^2 = Np_bq_b = M(1 - M/N)$

(note the variances are the same)

Suppose we make a series of n measurements with c measurements from the constant interval and b measurements from the balanced interval. Then we can get an estimator for p which we will denote $\hat{p} = c/n$ which is normally distributed as $Normal(p_a, \sigma^2/n)$ in case a) and which is normally distributed as $Normal(p_b, \sigma^2/n)$ in case b).

We want a sample size n such that these two distributions intersect at $p_a + 3\sigma/\sqrt{n}$ in case a) and $p_b - 3\sigma/\sqrt{n}$ in case b). This gives us a sample size n that is large enough that we determine case a) if $\hat{p} < p_a + 3\sigma$ and case b) if $\hat{p} > p_b - 3\sigma$.

We have

$$\begin{aligned}
M/N + 3\sqrt{M(1 - M/N)/n} &= (1 - M/N) - 3\sqrt{M(1 - M/N)/n} \\
\Rightarrow 6\sqrt{M(1 - M/N)/n} &= 1 - 2M/N \\
\Rightarrow n &= \frac{36M(1 - M/N)}{(1 - 2M/N)^2} \\
&\sim 36M \text{ when } M \ll N
\end{aligned}$$

In order for the Amplified-Haar transform to win we need the work factor of the above method to be worse than the work factor of the Amplified-Haar transform which is $O(\sqrt{N/2M})$. This gives the following inequality:

$$\begin{aligned}
\frac{36M(1 - M/N)}{(1 - 2M/N)^2} &> \sqrt{N/2M} \\
\Rightarrow \frac{1296M^2(1 - M/N)^2}{(1 - 2M/N)^4} &> N/2M \\
\Rightarrow M^3 &> \frac{N(1 - 2M/N)^4}{2592(1 - M/N)^2}
\end{aligned}$$

$$\Rightarrow M > \frac{N^{1/3}(1 - 2M/N)^{4/3}}{2592^{1/3}(1 - M/N)^{2/3}}$$

So we see that in this problem situation the Amplified-Haar transform wins if $M > N^{1/3}$ approximately speaking.

We should note that in the more general setting, if the set $L \setminus A$ is a mixture of balanced and constant components then just performing the Haar transform alone will not help to solve the problem of determining the nature of the set A because the probabilities of the set of A become impacted by the makeup of $L \setminus A$. The Amplified-Haar transform is not affected by this and is able to easily solve this more general situation.

Chapter 6: REFERENCES

The following references are directly relevant to the chapters of this thesis.

- [1] Nakahara and Ohmi, “Quantum Computing: From Linear Algebra to Physical Realizations”, CRC Press (2008).
- [2] S. Lomonaco, “Shor’s Quantum Factoring Algorithm,” AMS PSAPM, vol. 58, (2002), 161-179.
- [3] P. Shor, “Polynomial time algorithms for prime factorization and discrete logarithms on a quantum computer”, SIAM J. on Computing, 26(5) (1997) pp1484-1509 (quant-ph/9508027).
- [4] L. Grover, “A fast quantum mechanical search algorithm for database search”, Proceedings of the 28th Annual ACM Symposium on Theory of Computing (STOC 1996), (1996) 212-219.
- [5] Hardy and Wright “An Introduction to the Theory of Numbers”, Oxford Press Fifth Edition (1979).
- [6] S. Lomonaco and L. Kauffman, “Quantum Hidden Subgroup Algorithms: A Mathematical Perspective,” AMS CONM, vol. 305, (2002), 139-202.
- [7] S. Lomonaco, “Grover’s Quantum Search Algorithm,” AMS PSAPM, vol. 58, (2002), 181-192.

- [8] S. Lomonaco and L. Kauffman, "Is Grover's Algorithm a Quantum Hidden Subgroup Algorithm?," *Journal of Quantum Information Processing*, Vol. 6, No. 6, (2007), 461-476.
- [9] G. Brassard, P. Hoyer, M. Mosca and A. Tapp, "Quantum Amplitude Amplification and Estimation", *AMS CONM*, vol 305, (2002), 53-74.
- [10] M. Nielsen and I. Chuang, "Quantum Computation and Quantum Information", Cambridge University Press (2000).
- [11] P. Kaye, R. Laflamme and M. Mosca, "An Introduction to Quantum Computing", Oxford University Press (2007).
- [12] N. Yanofsky and M. Mannucci, "Quantum Computing For Computer Scientists", Cambridge University Press (2008).
- [13] S. Lomonaco, "A Lecture on Shor's Quantum Factoring Algorithm Version 1.1", quant-ph/0010034v1 9 Oct 2000.
- [14] Cornwell, D., "The amplified quantum Fourier transform: solving the local period problem", *Quantum Inf Process* (2013) 12: 1225-1253.
- [15] Donoho and Stark, "Uncertainty Principles and Signal Recovery", *SIAM J. Appl Math*, Vol 49, No 3, pp. 906-93 (1989)
- [16] Massar and Spindel, "Uncertainty Relations for the Discrete Fourier Transform", quant-ph, arXiv:0710.0723v2 (2008)
- [17] Loo, K, "Quantum Algorithm Uncertainty Principles", math-ph, arXiv:math-ph/0210007v2 (2004)

The following references are general references of relevance to the topics of this thesis.

1. S. Aaronson, “The Equivalence of Searching and Sampling”,
arXiv:1009.5104 [quant-ph]
2. S. Aaronson and A. Ambainis, “Quantum search of spatial regions”,
arXiv:quant-ph/0303041
3. S. Aaronson, “Quantum lower bound on recursive Fourier sampling”,
arXiv:quant-ph/0209060
4. G. Abal, R. Donangelo, M. Forets and R. Portugal, “Spatial quantum
search in a triangular network”, arXiv:1009.1422 [quant-ph]
5. A. Ambainis, “Quantum Algorithms”, arXiv:quant-ph/0504012.
6. A. Ambainis, A. Backurs, N. Nahimovs, R. Ozols and A. Rivosh, “Search
by quantum walks on two-dimensional grid without amplitude amplification”,
arXiv:1112.3337 [quant-ph]
7. A. Ambainis and A. Montanaro, “Quantum algorithms for search with
wildcards and combinatorial group testing”, arXiv:1210.1148 [quant-ph]
8. A. Ambainis, “Quantum search with variable times”,
arXiv:quant-ph/0609168
9. A. Ambainis, “A better lower bound for quantum algorithms searching
an ordered list”, arXiv:quant-ph/9902053
10. A. Barenco, A. Ekert, K. Suominen and P. Torma, “Approximate Fourier
transform and decoherence”, arXiv:quant-ph/9601018
11. M. Ben-Or and A. Hassidim, “Quantum search in an ordered list via
adaptive learning”
12. S. Berry and J. Wang, “Quantum Walk-based search and centrality”,

arXiv:1010.0764 [quant-ph]

13. E. Biham, O. Biham, D. Biron, M. Grassl and D. Lidar, “Grover’s quantum search algorithm for an arbitrary initial amplitude distribution”,
arXiv:quant-ph/9807027
14. O. Biham, D. Shapira and Y. Shimoni, “Analysis of Grover’s quantum search algorithm as a dynamical system”, arXiv:quant-ph/0307141
15. D. Biron, O. Biham, E. Biham, M. Grassl and D. Lidar, “Generalized Grover search algorithm for arbitrary initial amplitude distribution”, arXiv:quant-ph/9801066
16. C. Bowden, G. Chen, Z. Diao and A. Klappenecker, “The universality of the quantum Fourier transform in forming the basis of quantum computing algorithms”, arXiv:quant-ph/0007122
17. M. Boyer, G. Brassard, P. Hoyer and A. Tapp, “Tight bounds on quantum searching”, arXiv:quant-ph/9605034
18. G. Brassard, P. Hoyer and A. Tapp, “Quantum Counting”, arXiv:quant-ph/9805082.
19. G. Brassard, P. Hoyer, M. Mosca and A. Tapp, “Quantum Amplitude Amplification and Estimation”, AMS CONM, vol 305, (2002), 53-74.
20. H. Burhman and R. de Wolf, “Lower bounds for quantum search and derandomization”, arXiv:quant-ph/9811046
21. C. Cafaro and S. Mancini, “On Grover’s Search Algorithm from a Quantum Information Geometry Viewpoint”, arXiv.1110.6713 [quant-ph]
22. N. Cerf, L. Grover and C. Williams, “Nested quantum search and NP-complete problems”, arXiv:quant-ph/9806078
23. S. Chakraborty, S. Adhikari, “Non-classical Correlations in the Quan-

tum Search Algorithm”, arXiv:1302.6005v1 [quant-ph]

24. S. Chakraborty, S. Banerjee, S. Adhikari and A. Kumar, “Entanglement in the Grover’s Search Algorithm”, arXiv: 1305.4454 [quant-ph]

25. A. Chamoli and S. Masood, “Two-Dimensional Quantum Search Algorithm”, arXiv:1012.5629 [quant-ph]

26. A. Chamoli and M. Bhandari, “Success rate and entanglement evolution in search algorithm”, arXiv:quant-ph/0702221

27. J. Chappell, M. Lohe, L. Smekal, A. Iqbal and D. Abbot, “An improved formalism for the Grover search algorithm”, arXiv:1201.1707 [quant-ph]

28. J. Chen and H. Fan, “Quantum mechanical perspectives and generalization of the fractional Fourier transform”, arXiv:1307.6271

29. A. Childs and T. Lee, “Optimal quantum adversary lower bounds for ordered search”, arXiv:0708.3396

30. A. Childs, A. Landahl and P. Parrilo, “Improved quantum algorithms for the ordered search problem via semidefinite programming”,
arXiv:quant-ph/0608161

31. A. Childs and J. Goldstone, “Spatial search by quantum walk”,
arXiv:quant-ph/0306054

32. A. Childs, E. Deotto, E. Farhi, J. Goldstone, S. Gutmann, A. Landahl, “Quantum search by measurement”, arXiv:quant-ph/0204013

33. B. Choi and V. Korepin, “Quantum partial search of a database with several target items”, arXiv:quant-ph/0608106

34. B. Choi, T. Walker and S. Braunstein, “Sure success partial search”,

arXiv:quant-ph/0603136

35. R. Cleve and J. Watrous, "Fast parallel circuits for the quantum Fourier transform", arXiv:quant-ph/0006004

36. Cornwell, D., "The amplified quantum Fourier transform: solving the local period problem", Quantum Inf Process (2013) 12: 1225-1253.

37. D. Coppersmith, "An approximate Fourier transform useful in quantum factoring", arXiv:quant-ph/0201067

38. J.Cui and H. Fan, "Correlations in Grover Search", arXiv:0904:1703 [quant-ph]

39. Z. Diao. "Exactness of the Original Grover Search Algorithm", arXiv:1010.3652 [quant-ph]

40. S. Dolev, I. Pitowsky and B. Tamir, "Grover's quantum search algorithm and Diophantine approximation", arXiv:quant-ph/0507234

41. K. Dorai and D. Suter, "Efficient implementations of the quantum Fourier transform : an experimental perspective", arXiv:quant-ph/0211030

42. M. Falk, "Quantum Search on the Spatial Grid", arXiv:1303.4127 [quant-ph]

43. E. Farhi and S. Gutmann, "Quantum mechanical square root speedup in a structured search problem", arXiv:quant-ph/9711035

44. A. Fijany and C. Williams, "Quantum wavelet transforms: fast algorithms and complete circuits", arXiv:quant-ph/9809004

45. D. Floess, E. Andersson and M. Hillery, "Quantum algorithms for testing Boolean functions", arXiv:1006.1423v1 [quant-ph]

46. P. Gawron, J. Klemka and R. Winiarczyk, “Noise effects in the quantum search algorithm from the computational complexity point of view”,
arXiv:1108.1915 [quant-ph]
47. M. Gocwin, “On the complexity of searching maximum of a function on a quantum computer”, arXiv:quant-ph/0507060
48. R. Griffiths and C. Niu, “Semiclassical Fourier transform for quantum computation”, arXiv:quant-ph/9511007
49. L. Grover, ”A fast quantum mechanical search algorithm for database search”, Proceedings of the 28th Annual ACM Symposium on Theory of Computing (STOC 1996), (1996) 212-219.
50. L. Grover, “A fast quantum mechanical search algorithm for database search”, arXiv:quant-ph/9605043
51. L. Grover, “Quantum computers can search arbitrarily large databases by a single query”, arXiv:quant-ph/9706005v3.
52. L. Grover,”Quantum Search on Structured Problems”,
arXiv:quant-ph/9802035
53. L. Grover, “Searching with quantum computers”,
arXiv:quant-ph/0011118
54. L. Grover,”Tradeoffs in the Quantum Search Algorithm”,arXiv:quant-ph/0201152.
55. L. Grover,”Quantum Searching amidst Uncertainty”,
arXiv:quant-ph/0507116.
56. L. Grover,”Superlinear amplitude amplification”,
arXiv:0806.0154 [quant-ph]

57. L. Grover, “A different kind of quantum search”,
arXiv:quant-ph/0503205
58. L. Grover, “How fast can a quantum computer search”,arXiv:quant-ph/9809029
59. L. Grover, “Quantum computers can search rapidly by using almost
any transformation”,arXiv:quant-ph/9712011
60. L. Grover, “Quantum mechanics helps in searching for a needle in a
haystack”,arXiv:quant-ph/9706033
61. L. Grover and J Radhakrishnan,”Quantum search for multiple items
using parallel queries”,arXiv:quant-ph/0407217.
62. L. Grover and J. Radhakrishnan, “Is partial quantum search of a
database any easier”, arXiv:quant-ph/0407122
63. L. Grover and T.Rudolph,”Creating superpositions that correspond to
efficiently integrable probability distributions”,arXiv:quant-ph/0208112.
64. L. Grover, A. Patel and T. Tulsi, “Quantum algorithms with fixed
points: the case of database search”, arXiv:quant-ph/0603132
65. L. Gyongyosi and S. Imre, “An improvement in quantum Fourier trans-
form”, arXiv:1207.4464
66. L.Hales, “The quantum Fourier transform and extensions of the Abelian
hidden subgroup problem”, arXiv:quant-ph/0212002
67. L. Hales and S. Hallgren,”Sampling Fourier transforms on different
domains”,arXiv:quant-ph/9812060
68. Hardy and Wright ”An Introduction to the Theory of Numbers”, Ox-
ford Press Fifth Edition (1979).

69. B. Hein and G. Tanner, “Quantum search algorithms on a regular lattice”, arXiv:1005:3676 [quant-ph]
70. B. Hein and G. Tanner, “Quantum search algorithms on the hypercube”, arXiv:0906.3094 [quant-ph]
71. M. Hillery, D. Reitzner and V. Bunek, “Searching via walking: How to find a marked subgraph of a graph using quantum walks”, arXiv:0911:1102 [quant-ph]
72. T. Hogg, “Single-Step Quantum Search Using Problem Structure”, arXiv:quant-ph/9812049.
73. T. Hogg, “A framework for structured quantum search”, arXiv:quant-ph/9701013
74. T. Hogg, “A framework for quantum search heuristics”, arXiv:quant-ph/9611004
75. T. Hogg and M. Yanik, “Local search methods for quantum computers”, arXiv:quant-ph/9802043
76. P. Hoyer, J. Neerbek and Y. Shi, “Quantum complexities of ordered searching, sorting and element distinctness”, arXiv:quant-ph/0102078
77. J. Hsieh, C. Li, J. Lin and D. Chu, “Formulation of a family of sure success quantum search algorithms”, arXiv:quant-ph/0210201
78. M. Hunziker, D. Meyer, J. Park, J. Pommersheim and M. Rothstein, “The Geometry of Quantum Learning”, arXiv:quant-ph/0309059.
79. N. Ilano, C. Villagonzalo and R. Banzon, “Analysis of the damped quantum search and its application to the one-dimensional Ising system”, arXiv:1208.5509v1 [quant-ph]
80. N. Ilano, C. Villagonzalo and R. Banzon, “Optimization of the damped

quantum search”, arXiv:1208.5475 [quant-ph]

81. L. Ip, “Solving shift problems and hidden coset problem using the Fourier transform”, arXiv:quant-ph/0205034

82. S. Iriyama, M. Ohya, I.V. Volovich, “On Quantum Algorithm for Binary Search and its Computational Complexity”, arXiv:1306.5039v1 [quant-ph]

83. S. Ivanov, H. Tonchev and N. Vitanov, “Time-efficient implementation of quantum search with qudits”, arXiv:1209.4489 [quant-ph]

84. R. Josza, “Searching in Grover’s algorithm”, arXiv:quant-ph/9901021

85. R. Josza, “Quantum algorithms and the Fourier transform”, arXiv:quant-ph/9707033

86. P. Kaye, R. Laflamme and M. Mosca, ”An Introduction to Quantum Computing”, Oxford University Press (2007).

87. V. Korepin and Y. Xu, “Binary quantum search”, arXiv:0705.0777

88. V. Korepin and J. Liao, “Quest for fast partial search algorithm”, arXiv:quant-ph/0510179

89. V. Korepin and L. Grover, “Simple algorithm for partial quantum search”, arXiv:quant-ph/0504157

90. V. Korepin, “Optimization of partial search”, arXiv:quant-ph/0503238

91. K. Kumar and G. Paraoanu, “A quantum no reflection theorem and the speeding up of Grover’s search algorithm”, arXiv:1105.4032 [quant-ph]

92. T. Laarhoven, M. Mosca and J. van de Pol, “Solving the Shortest Vector Problem in Lattices Faster Using Quantum Search”, arXiv:1301.6176v1 [quant-ph]

93. C. Lavor, L. Manssur and R. Portugal, “Grover’s algorithm: quantum

database search”, arXiv:quant-ph/03010179

94. J. Lee, H. Lee and M. Hillery, “Searches on star graphs and equivalent oracle problems”, arXiv:1102.5480 [quant-ph]

95. T. Lee, F. Magniez and M. Santha, “Improved Quantum Query Algorithms for Triangle Finding and Associativity Testing”, arXiv:1210.1014v1 [quant-ph]

96. S. Lloyd, “Quantum search without entanglement”,
arXiv:quant-ph/9903057

97. S. Lomonaco, ”Grover’s Quantum Search Algorithm,” AMS PSAPM, vol. 58, (2002), 181-192.

98. S. Lomonaco, ”Shor’s Quantum Factoring Algorithm,” AMS PSAPM, vol. 58, (2002), 161-179.

99. S. Lomonaco, ”A Lecture on Shor’s Quantum Factoring Algorithm Version 1.1”, quant-ph/0010034v1 9 Oct 2000.

100. S. Lomonaco and L. Kauffman, ”Quantum Hidden Subgroup Algorithms: A Mathematical Perspective,” AMS CONM, vol. 305, (2002), 139-202.

101. S. Lomonaco and L. Kauffman, ”Is Grover’s Algorithm a Quantum Hidden Subgroup Algorithm?,” Journal of Quantum Information Processing, Vol. 6, No. 6, (2007), 461-476.

102. C. Lomont, “A quantum Fourier transform algorithm”, arXiv:quant-ph/0404060

103. N. Lovett, M. Everitt, R. Heath and V. Kendon, “The quantum walk search algorithm: Factors affecting efficiency”, arXiv:1110.4366v2 [quant-ph]

104. N. Lovett, M. Everitt, M. Trevers, D. Mosby, D. Stockton and V.

Kendon, “Spatial search using the discrete time quantum walk”, arXiv:1010.4705 [quant-ph]

105. F. Magniez, A. Nayak, J. Roland and M. Santha, “Search via quantum walk”, arXiv:quant-ph/0608026

106. A. Mani and C. Patvardhan, “A Fast measurement based fixed-point Quantum Search Algorithm”, arXiv:1102.2332 [quant-ph]

107. A. Mani and C. Patvardhan, “A Fast fixed-point Quantum Search Algorithm by using Disentanglement and Measurement”, arXiv:1203.3178 [quant-ph]

108. F. Marquezino, R. Portugal and S. Boettcher, “Quantum Search Algorithms on Hierarchical Networks”, arXiv:1205.0529 [quant-ph]

109. D. Meyer and T. Wong, “Nonlinear Quantum Search Using the Gross-Pitaevskii Equation”, arXiv:1303.0371v3 [quant-ph]

110. F. Marquezino, R. Portugal and S. Boettcher, “Spatial Search Algorithms on Hanoi Networks”, arXiv:1209.2871 [quant-ph]

111. A. Mizel, “Critically damped quantum search”, arXiv:0810.0470 [quant-ph]

112. A. Montanaro, “Quantum search with advice”, arXiv:0908.3066 [quant-ph]

113. A. Montanaro, “Quantum search of partially ordered sets”, arXiv:quant-ph/0702196

114. C. Moore, D. Rockmore and A. Russell, “Generic quantum Fourier transforms”, arXiv:quant-ph/0304064

115. C. Moore, D. Rockmore, A. Russell and L. Schulman, “The power of

strong Fourier sampling: quantum algorithms for affine groups and hidden shifts”,
arXiv:quant-ph/0503095

- 116. M. Mosca,”Quantum Algorithms”,arXiv:0808.0369 [quant-ph]
- 117. M. Mosca and C. Zalka,”Exact quantum Fourier transforms and discrete logarithm algorithms”,arXiv:quant-ph/0301093.
- 118. Y. Most, Y. Shimoni and O. Biham, “Entanglement of periodic states, the quantum Fourier transform and Shor’s factoring algorithm”, arXiv:1001:3145
- 119. Nakahara and Ohmi, ”Quantum Computing: From Linear Algebra to Physical Realizations”, CRC Press (2008).
- 120. A. Nesterov and G. Berman, “Quantum search using non-Hermitian adiabatic evolution”,arXiv:1208.4642 [quant-ph]
- 121. M. Nielsen and I. Chuang, ”Quantum Computation and Quantum Information”, Cambridge University Press (2000).
- 122. R. Orus, J. Latorre and M. Martin-Delgado,”Natural majorisation of the quantum Fourier transform in phase-estimation algorithms”, arXiv:quant-ph/0206134
- 123. S. Parasa and K. Eswaran, “Quantum pseudo fractional Fourier transform and its application to quntum phase estimation”,arXiv:0906.1033
- 124. A. Patel, “Quantum Algorithms: Database Search and its Variations”, arXiv:1102.2058 [quant-ph]
- 125. A. Patel, K. Raghunathan and M. Rahaman, “Search on a Hypercubic Lattice through a quantum random walk: II. $d=2$ ”, arXiv:1003.5664 [quant-ph]
- 126. A. Patel and M. Rahaman, “Search on a Hypercubic Lattice through a quantum random walk: I. $d>2$ ”, arXiv:1003.0065 [quant-ph]

127. A. Perez, “Non adiabatic quantum search algorithms”, arXiv:0706.1139
128. A. Pittenger and M. Rubin, “Complete separability and Fourier representations of n-qubit states”, arXiv:quant-ph/9912116
129. A. Pittenger and M. Rubin, “Separability and Fourier representations of density matrices”, arXiv:quant-ph/0001014
130. V. Potocek, A. Gabris, T. Kiss and I. Jex, “Optimized quantum random-walk search algorithms”, arXiv:0805.4347.
131. R. Qu, J. Wang, Z. Li, Y. Bao and X. Cao, “Multipartite entanglement and Grover’s search algorithm”, arXiv:1210.3418
132. D. Bhaktavatsala Rao and K. Molmer, “Effect of qubit losses on Grover’s quantum search algorithm”, arXiv:1209.0637 [quant-ph]
133. R. Ramos, P. de Sousa, D. Oliveira, “Solving mathematical problems with quantum search algorithm”, arXiv:quant-ph/0605003
134. O. Regev and L. Schiff, “Impossibility of a Quantum Speed-up with a Faulty Oracle”, arXiv:1202.1027v1 [quant-ph]
135. H. Roehrig, “Searching an ordered list on a quantum computer”, arXiv:quant-ph/9812061
136. M. Rossi, D. Brus and C. Macchiavello, “Scale invariance of entanglement dynamics in Grover’s quantum search algorithm”, arXiv:1205.3000 [quant-ph]
137. P. Rungta, “The quadratic speedup in Grover’s search algorithm from the entanglement perspective”, arXiv:0707.1410
138. M. Santha, “Quantum walk based search algorithms”, arXiv:0808.0059 [quant-ph]

139. D. Shapira, S. Mozes and O. Biham, "The effect of unitary noise on Grover's quantum search algorithm", arXiv:quant-ph/0307142
140. N. Shenvi, K. Brown and K. Whaley, "Effects of noisy oracle on search algorithm complexity". arXiv:quant-ph/0304138
141. N. Shenvi, J. Kempe and K. Whaley, "A quantum random walk search algorithm", arXiv:quant-ph/0210064
142. P. Shor, "Polynomial time algorithms for prime factorization and discrete logarithms on a quantum computer", SIAM J. on Computing, 26(5) (1997) pp1484-1509 (arXiv:quant-ph/9508027).
143. P. Shor, "Introduction to Quantum Algorithms", arXiv:quant-ph/0005003.
144. R. Sufiani and N. Bahari, "Quantum search in structured database using local adiabatic evolution and spectral methods", arXiv:1208.0262 [quant-ph]
145. R. Tucci, "Quantum fast Fourier transform viewed as a special case of recursive application of cosine-sine decomposition", arXiv:quant-ph/0411097
146. A. Tulsi, "Optimal quantum searching to find a common element of two sets", arXiv:1210.04648 [quant-ph]
147. A. Tulsi, "General framework for quantum search algorithms", arXiv:0806.1257 [quant-ph]
148. A. Tulsi, "Faster quantum walk algorithm for the two dimensional spatial search", arXiv:0801.0497
149. A. Tulsi, "Quantum computers can search rapidly using almost any selective transformation", arXiv:0711.4299

150. J. Tyson, "Operator-Schmidt decomposition of the quantum Fourier transform on $C^{N_1} \otimes C^{N_2}$ ", arXiv:quant-ph/0210100
151. P.Vrana, D. Reeb, D. Reitzner and M. Wolf, "Fault-ignorant Quantum Search", arXiv:1307.0771v1 [quant-ph]
152. N. Yanofsky and M. Mannucci, "Quantum Computing For Computer Scientists", Cambridge University Press (2008).
153. A. Younes, "Strength and Weakness in Grover's Quantum Search Algorithm", arXiv:0811.4481 [quant-ph]
154. A. Younes, "Constant-Time Quantum Search Algorithm for the Unstructured Search Problem", arXiv:08114247 [quant-ph]
155. A. Younes, "Fixed phase quantum search algorithms", arXiv:0704.1585
156. A. Younes, J. Rowe and J. Miller, "A hybrid quantum search algorithm: a fast quantum algorithm for multiple matches", arXiv:quant-ph/0311171
157. C. Zalka, "A Grover-based quantum search of optimal order for an unknown number of marked elements", arXiv:quant-ph/9902049
158. C. Zalka, "Grover's quantum searching algorithm is optimal", arXiv:quant-ph/9711070
159. M. Zakaria, "Binary Subdivision for Quantum Search", arXiv:1101.4703 [quant-ph]

The following is a list of books:

1. A. Aezel, "Entanglement", Plume, 2001
2. Y. Aharonov and D. Rohrlich, "Quantum paradoxes", Wiley, 2009
3. G. Van Assche, "Quantum cryptography and secret-key distillation",

Cambridge,2006

4. J. Audretsch (Ed), "Entangled world".Wiley, 2002
5. J. Baggot, "The meaning of quantum theory", Oxford,1994
6. I. Bengtsson and K. Zyczkowski, " Geometry of quantum states", Cambridge,2008
7. D. Bernstein, J. Buchmann and E. Dahmen (Eds), "Post-quantum cryptography", Springer, 2009
8. D. Bouwmeester, A. Ekert, A. Zeilinger (Eds), "The physics of quantum information", Springer,2000
9. G. Chen, L. Kauffman and S. Lomonaco, "Mathematics of quantum computation and quantum technology", Chapman & Hall,2008
10. I. Daubechies, "Ten lectures on wavelets",SIAM Vol 61, 2006
11. L. Debnath, "Wavelet transforms and their applications", Birkhauser, 2002
12. P. Dirac, "The principles of quantum mechanics", Oxford, 1999
13. R. Feynman, "QED: The strange theory of light and matter", Princeton, 1985
14. G. Gamow, "Thirty years that shook physics: the story of quantum theory",Dover, 1985
15. J. Gruska, "Quantum computing", McGraw Hill, 1999
16. M. Hirvensalo, "Quantum computing", Springer, 2004
17. P. Kaye, R. LaFlamme and M. Mosca, "An Introduction to Quantum Computing", OUP 2007.

18. M. Kumar, "Quantum: Einstein, Bohr and the great debate about the nature of reality", Norton, 2008
19. F. Laloe, "Do we really understand quantum mechanics", Cambridge, 2013
20. S. Lomonaco (Ed.), "Quantum Computation: A grand mathematical challenge for the twenty first century and the millennium", AMS Vol 58, 2000
21. S. Lomonaco (Ed.), "Quantum Computation and Information", AMS 305
22. D. McMahon, "Quantum computing explained", Wiley, 2008
23. N. Mermin, "Quantum computer science – An introduction", Cambridge, 2007
24. M. Nakahara and T. Ohmi, "Quantum computing: from linear algebra to physical realizations", CRC Press, 2008
25. M. Nielsen and I. Chuang, "Quantum computation and quantum information", Cambridge 2000
26. Y. Nievergelt, "Wavelets made easy", Birkhauser, 2001
27. J. Polkinghorne, "The quantum world", Princeton, 1989
28. R. Portugal, "Quantum walks and search algorithms", Springer, 2013
29. A. Rae, "Quantum Physics: Illusion or Reality", Canto, 2005
30. E. Rieffel and W. Polak, "Quantum computing: A gentle introduction", MIT, 2011
31. A. Terras, "Fourier Analysis on Finite Groups and Applications", LMS vol 43, 2001

32. P. Van Fleet,"Discrete Wavelet Transformations",Wiley,2008
33. J. Walker, "A primer on Wavelets and their scientific applications",
Chapman & Hall, 2008
34. D. Walnut,"An introduction to wavelet analysis", Birkhauser, 2004
35. R. Wang,"Introduction to orthogonal transforms",Cambridge, 2012
36. A. Whitaker, "The new quantum age",Oxford, 2012
37. A. Whitaker,"Einstein, Bohr and the quantum dilemma",
Cambridge,2006
38. C. Williams, "Explorations in Quantum Computing", Springer 2011
39. N. Yanofsky and M. Mannucci, "Quantum computing for computer
scientists",Cambridge, 2008

